International Report on Internet Censorship

International Focus Programme on Law and Technology

Final Report of the International Legal Research Group on Internet Censorship (eds)

International Report on Internet Censorship

International Focus Programme on Law and Technology

International Report on Internet Censorship

International Focus Programme on Law and Technology

Final Report of the International Legal Research Group on Internet Censorship (eds)

The European Law Students' Association

International Report on Internet Censorship
International Focus Programme on Law and Technology
Final Report of the International Legal Research Group on Internet Censorship (eds)

ISBN: 978-94-6240-645-2 (paperback)
ISBN: 978-94-6240-646-9 (e-version)

European Law Students' Association (ELSA)
Boulevard Général Jacques 239
1050 Brussels
Belgium

E-Mail: academicactivities@elsa.org
Website: https://elsa.org

Published by:
Wolf Legal Publishers
Gasthuisvelden 11
4811 VX Breda
The Netherlands

E-Mail: info@wolfpublishers.nl
Website: www.wolfpublishers.eu
Website: www.discoverlawbooks.com

International Legal Research Group on Internet Censorship

The European Law Students' Association (ELSA)

Editor in Chief

Sarah Ikast Kristoffersen

Vice President in charge of Academic Activities

International Board of ELSA 2019/2020

Deputy Editor in Chief

Nikola Ćirić

Director for Legal Writing

ELSA International 2019/2020

International Coordinator

Fani Dimoska

ELSA International 2019/2020

International Linguistic Editor

Vanya Rakesh

ELSA International 2019/2020

International Technical Editor

Oļegs Sedjakins

ELSA International 2019/2020

2020

Foreword

By Patrick Penninckx, Head of Information Society Department, Council of Europe

This report discusses one of the most important questions in open societies today: how do we strike the right balance between freedoms and protections in the online environment?

Freedom of expression is a fundamental human right, essential to the functioning of democratic societies and the human rights system. It is listed amongst the basic rights in all international and regional human rights treaties. Article 10 of the European Convention on Human Rights protects the freedom to hold opinions and to receive and impart information and ideas without interference by public authorities, regardless of frontiers.

However, freedom of expression is not an absolute right. Not all restrictions constitute censorship. Speech may be restricted if this is prescribed by law, necessary in a democratic society and proportionate to a legitimate aim. The latter may include national security, public health or the protection of the rights of others. The COVID-19 pandemic serves as a vivid example of a public health crisis demanding decisive government action, including as far as proportionate restrictions to the exercise of rights are concerned.

Yet, what is proportionate? Determining what speech may be restricted and what not is highly complex. It has been the subject of court deliberations and public debates over centuries. The online environment makes this already difficult task even more complicated: there are added uncertainties around territorial jurisdiction, such as in the case of search engines or global social networks that are registered abroad. Illegal content may either go ignored or go viral, making it difficult to assess its actual harm. Harmful speech may travel instantaneously, with content banned in one location finding free expression elsewhere, in a different country or a different virtual space. Accountability is often elusive as users, whether individuals or legal entities, may hide behind pseudonymous accounts.

Any regulatory or other measure to curb illegal speech online must take these aspects into account. In addition, it must consider the crucial role that intermediaries, including internet access providers, social networks and search engines, play in facilitating communication. This is all the more so as few, large entities have come to dominate the market in a manner that allows them to shape the principle modes of public communication. The power of such intermediaries as protagonists of online expression makes it imperative to assess very carefully

their role and impact on freedom of expression and other human rights, as well as their corresponding duties and responsibilities.

Faced with growing pressure from governments and the public, the major social media platforms are increasingly committing to policing the online environment and removing illegal content. This in turn raises serious concerns regarding their possible overreach and the absence of judicial supervision. Are we facilitating private censorship of legal speech?

The Council of Europe has been supporting its 47 member States in the difficult task of governing and regulating the online environment for decades. Its 'Comparative Study on Filtering, Blocking and Take-down of Illegal Content on the Internet', published in 2016, revealed a broad variety of approaches across Europe, as well as important challenges. Since then, the situation has further evolved; infrastructure, scale and nature of the internet as essential tool of everyday life today confront us with new tasks.

The present report, which examines the way that more than 20 European jurisdictions have been weighing freedom of expression online against other rights, constitutes a rich source of information also for the Council of Europe. As an organisation we remain committed to supporting our member States in finding effective solutions to today's evolving questions: how can we comprehensively and effectively combat hate speech and other forms of illegal content online? How do we ensure that legal speech is protected against automated forms of content moderation? How can law enforcement cooperate more efficiently across borders in order to promote a safer internet? How do we protect our privacy in a world where algorithmic systems and AI have a growing command over our digital identities?

The COVID-19 pandemic and the diverse responses taken by governments to contain and resolve the crisis only amplify the need for solutions to these important questions.

I therefore highly welcome this important contribution to a field that requires the continued curiosity, scrutiny and intelligence of legal researchers across Europe. And I am confident that this report will serve as a reference point for future initiatives in Europe and beyond, aimed at promoting an open internet without censorship.

Introduction

1. About ELSA

ELSA is a non-political, non-governmental, non-profit making, independent organisation which is run by and for students. ELSA has 44 member countries and 69,000 students represented at across 375 faculties. The association was founded in 1981 by 5 law students from Poland, Austria, West Germany and Hungary. Since then, ELSA has aimed to unite students from all around Europe, provide a channel for the exchange of ideas and opportunities for law students and young lawyers to become internationally minded and professionally skilled. Our focus is to encourage individuals to act for the good of society in order to realise our vision: "A just world in which there is respect for human dignity and cultural diversity". You can find more information on elsa.org.

2. International Legal Research Groups in ELSA

Through an International Legal Research Group (ILRG) a group of law students and young lawyers carry out research on a specified topic of law with the aim to make their conclusions publicly accessible. Legal research has always been one of the main aims of ELSA. When ELSA was created as a platform for European cooperation between law students in the 1980s, sharing experience and knowledge was the main purpose of our organisation. In the 1990s, our predecessors made huge strides and built a strong association with a special focus on international exchange. In the 2000s, young students from Western to Eastern Europe were facing immense changes in their legal systems. Our members were part of major legal developments such as the EU expansion and the implementation of EU Law. To illustrate, the outcome of the ELSA PINIL (Project on International Criminal Court National Implementation Legislation) has been the largest international criminal law research in Europe. In fact, the final country reports have been used as a basis for establishing new legislation in many European countries. The results of our more recent ILRGs are available electronically. ELSA for Children (2012) was published on Council of Europe's web pages and resulted in a follow up LRG (2014) together with, among others, Missing Children Europe. In 2013, ELSA was involved in Council of Europe's 'No Hate Speech Movement'. The final report resulted in a concluding conference in Oslo that same year and has received a lot of interest from academics and activists in the field of discrimination and freedom of speech. The results of the ILRG conference, a guideline, have even been translated into Japanese and were presented at the Council of Europe and UNESCO.

3. The International Legal Research Group on Internet Censorship

The International Legal Research Group on Internet Censorship has researched issues such as taking down and filtering internet content, online hate speech and liability of internet intermediaries across 24 European jurisdictions and published this in this Final Report.

The final report explores the legal background of an awareness survey on freedom of expression online run by ELSA and containing more than 1,000 unique responses. This survey found, among others, that almost 80% of the respondents have experienced fake news online while more than 67% have experienced online hate speech.

The final report falls under the implementation of ELSA's International Focus Programme on the interplay between Law and Technology. This focus programme seeks to explore how technology and technological developments may affect law and how law and regulation may affect the realisation of the full potential of technology and innovation.

Acknowledgements

This International Legal Research Group came into existence thanks to the immense effort from several individuals, from national level all through the international, and from the professional to the student level. Firstly, the National Coordinators for managing their National Research Groups and submitting the reports, their respective teams for doing the wonderful groundwork of actually researching and writing – there would be no publication without your contributions. Secondly, the Patron of the ILRG, Patrick Penninckx from the Council of Europe, as well as the Academic Board which drafted the Academic Framework and reviewed the quality of the report; Gavin Sutter, Guido Westkamp, William Echikson, Katerina Iliadou and Snjezana Vasiljevic. Finally, we wish to thank our external partners, including Queen Mary University of London and Wolf Publishers. The quality of this publication depends heavily on their extensive support and advice. Therefore, we extend our sincerest gratitude to these partners. This report was published in a time where protection of free speech on the internet has never been more important; the global pandemic necessitates unbiased information for all citizens, and online hate speech has unfortunately been on a rise across the continent. While challenges will always remain, we believe that we are one step closer to creating a just world through this collaborative and comparative effort.

Thankfully yours,

Sarah, Nikola, Fani, Vanya and Oļegs

The International Coordination Team of the
International Legal Research Group on Internet Censorship

Table of contents

Academic Framework

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?
2. Which legislation on the issue of blocking and takedown of internet content does your country have?
3. On which ground may internet content be blocked/filtered or taken down/removed in your country?
4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?
5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?
6. How does your country regulate the liability of internet intermediaries?
7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?
8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?
9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?
10. How do you rank the access to freedom of expression online in your country?
11. How do you overall assess the legal situation in your country regarding internet censorship?

ELSA Albania

Contributors

National Coordinator

Klea Sena

National Academic Coordinator

Klea Sena

National Researchers

Esmeralda Dida

Glen Mebelli

Kris Hasa

Luizita Voda

National Academic Supervisor

Arlind Ahmetaj

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

1.1. Albanian Constitution on freedom of expression and right to information.

As the country changed its form of government from a communist regime to a democratic one in 1991, freedom of expression and the right to information are relatively new concepts in Albanian constitutional law. In the previous rule, freedom of expression was one of the most infringed freedoms in the country, and people were often sentenced for a penal act called 'agitation and propaganda'. As of 1991, the Albanian Parliament adopted the Law No.7491 Date 29 April 1991 'On the Main Constitutional Dispositions' (Ligji Nr.7491, Datë 29 April 1991 'Për dispozitat kryesore kushtetuese') making Albania a democratic country. This law served as a temporary constitution, and even though it did not mention the freedom of expression explicitly, in its text in Article 4 provided that the Republic of Albania recognizes and guarantees the human rights and fundamental freedoms, as well as rights of national minorities, accepted in international documents. Even though the text of this law was not exhaustive in protecting human rights, it was enough to correct some of the injustice that the communist rule made people suffer and it set the first stone in building a proper legal framework regarding the protection of the freedom of speech.

The current constitution in Albania was adopted in 1998, and it includes freedom of expression as a constitutional freedom provided in Article 22. It guarantees the freedom of expression and also the freedom of press, radio and television. It prohibits the prior censorship to means of communications. It provides that the law may require the granting of authorization for the operation of radio and television channels.

The Albanian Constitution was adopted in 1998, and even though it has been amended six times in the years 2007, 2008, 2012, 2015 and 2016, this article has remained untouched. The second paragraph of the aforementioned article is focused on the press, radio and television, leaving internet communication means unmentioned. However, this aspect is covered by the third paragraph, which prohibits prior censorship of means of communication, which shall include the internet. Despite this fact, it would be efficient to amend the second paragraph so the Constitution would guarantee freedom of internet communication as well.

Article 22 must be interpreted together with Article 23 of the Constitution, which provides that the right to information is guaranteed and that everyone has the right, in compliance with law, to obtain information about the activity of state organs, and of persons who exercise state functions. Everyone is given the possibility to attend meetings of elected collective organs.

The Constitutional Court of Albania as the "guardian" of the Constitution also states the importance of freedom of expression in its Decision No. 16, Date 11 November 2004 stating that exchange of ideas and free information are among the most important and effective means of controlling democracy as a form of government. Through them, state power becomes more transparent, more efficient and closer to the citizen. Freedom of expression is also a necessary basis and a prerequisite for the enjoyment of a range of other fundamental rights and freedoms. For this reason, the practical application of this right in each case requires a very broad understanding and interpretation.

There is a difference between the freedom of radio and television and freedom of press. The constitution allows the law to require the granting of authorization for the operation of radio and television channels, but such requirement does not exist in the case of press.

1.2. Other domestic laws on freedom of expression and right to information

In accordance with the Constitution, the Law No.8410 Date 30 September 1998 'On the public and private radio and television in the Republic of Albania' (Ligji Nr.8410 Datë 30 September 1998 'Për radion dhe televizionin publik dhe privat në Republikën e Shqipërisë') provides in the second paragraph of Article 35 that in censorship is not allowed in radio and television programs.

Furthermore, censorship is not explicitly mentioned in Law No.7756 Date 11 October 1993 'On the press' (Ligji Nr.7756 Datë 11 October 1993 'Për Shtypin'), however, it is only Article in force provides that the press is free, and freedom of the press is protected by law.[1]

The abovementioned law was amended in 1997. The original text contained a broader Article 1, while in 1997 the rest of its sentences were repealed, together with the rest of the dispositions of the law.

This abrogation has left Albania without a detailed law to regulate the press activities further.

---

1 Article 1 of Law No.7756 Date 11.10.1993 "On the Press", amended [Ligji Nr.7756 Datë 11.10.1993 "Për Shtypin", i ndryshuar].

Another law granting the freedom of expression in Albania is Law No.97/2013 'On the audiovisual media in the Republic of Albania' (Ligji Nr.97/2013 'Për mediat audiovizive në Republikën e Shqipërisë'). Some of the principles that govern this law are:

- Freedom of the audiovisual transmissions;
- Impartiality in granting the right for information, political persuasion and religion, personality, dignity and other fundamental human rights, as well as the moral and legal rights and interests for the protection of children;
- Respect to the constitutional order, sovereignty and national integrity;
- Granting of objective and impartial information to the public;
- Granting the right for every citizen to receive service of audio and/or audiovisual from the operators of audiovisual services, exercising activity in the territory of Republic of Albania.[2]

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

2.1. No specific legislation

There is no specific legislation currently into effect in Albania that targets blocking and taking down of content on the internet. However, legislative initiatives that specifically regulate the issue have been proposed by the Council of Ministers and are currently being reviewed in the Parliament of Albania after being passed into law and then immediately turned back for review by Presidential Decree[3] without coming into effect.

The abovementioned draft law has gotten negative feedback from some journalists and a number of non - profit organizations that work on the field of human rights and has been considered controversial by many. Moreover, the Monitoring Committee of the Parliamentary Assembly of the Council of Europe requested an opinion of the Venice Commission concerning this law.[4]

That being said, as of this date, no specific legislation in regard to blocking and taking down internet content is yet applicable in Albania.

---

2 Article 4 of Law No.97/2013 "On the audiovisual media in the Republic of Albania" [Ligji Nr.97/2013 "Për mediat audiovizive në Republikën e Shqipërisë"].

3 Decree no. 11413, dated 11 January 2020 and Decree no. 11414, dated 11 January 2020.

4 Council of Europe, Request for opinion by PACE, <https://www.venice.coe.int/webforms/events/?id=2882> accessed 25 July 2020.

2.2. Case law on the topic

Neither in Albanian Constitutional Court nor European Court of Human Rights has there ever been a case with Albania as a party, regarding blocking or takedown of internet content. Relevant benchmark cases with other parties, regarding the issue, that can be somewhat used to draw comparisons with regulations in Albania are mentioned below on question number 3.

2.3. Legislation on the topic

Regulations concerning the issue of content filtering can be found spread over several kinds of sources whether that be ratified international treaties, laws or normative acts. Keeping in mind the hierarchy of the norms[5] in Albania, these sources will be listed legislation below and the mechanisms used by each will be explained thoroughly on research question 3.

Each legislation and the mechanisms used by each source to regulate the issue shall be explained in detail in question number 3. It should be noted that all laws listed below do protect the freedom of expression and their filtering mechanisms are in accordance with Article 17 of the Albanian Constitution which strictly provides the conditions under which a fundamental human right can be limited. These conditions are:

- only by law;
- to be in the public interest or for the protection of the rights of others;
- to be in proportion to the situation that has dictated it;
- to not infringe the essence of the right;
- to not exceed the limitation provided for in the European Convention of Human Rights.

The filtering mechanisms, explained in question 3, are all prescribed by law, all of which awake a public interest such as protection from cybercrime, protection for victims of sexual abuse or victims of xenophobia, protection from terrorist attacks or preventing severe consequences of defamation. They seem to pass the test of proportionality and do not exceed limitations provided for in the Convention, as analysed in a number of decisions of the European Court of Human Rights, one of those being *Handyside v United Kingdom,*[6] which serves as a

5 Article 116, Constitution of the Republic of Albania "Normative acts that are effective in the entire territory of the Republic of Albania are: a. the Constitution; b. ratified international agreements; c. the laws; ç. normative acts of the Council of Ministers".

6 Handyside v The United Kingdom, application number 5493/72, judgement on 7 December 1976.

landmark judgement concerning the analysis of limitation criteria for Article 10 of the Convention, freedom of expression.

Ratified international treaties:

- European Convention on Cybercrime[7]
- Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems[8]
- The Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse[9]
- Optional Protocol to the Convention on the Rights of Children, the sale of children, child prostitution and child pornography[10]
- Council of Europe Convention on the Prevention of Terrorism[11]

Laws:

- Penal Code of the Republic of Albania[12]
- Civil Code of the Republic of Albania[13]
- Law on protection of personal data, as amended[14]
- Law on copyright and other rights related to it, as amended[15]

Normative acts:

- 'Cyber Defence Strategy 2018-2020' – Ministry of Defence[16]

---

7 Adopted by Law no. 8888, date 24 April 2002.
8 Approved by Law no. 9262, date 29 July 2004.
9 Approved by Law no. 10071, date 9 February 2009.
10 Approved by Law no. 9834, date 22 November 2007.
11 Approved by Law no. 9641, date 20 November 2006.
12 Publication of the Centre for Official Publications, Criminal Code of the Republic of Albania <https://qbz.gov.al/preview/a2b117e6-69b2-4355-aa49-78967c31bf4d> 2019.
13 Publication of the Centre for Official Publications, Civil Code of the Republic of Albania <https://qbz.gov.al/preview/f010097e-d6c8-402f-8f10-d9b60af94744> 2019.
14 Additions and Amendments to Law No. 9887, dated 10 March 2008 "On Personal Data Protection" <https://qbz.gov.al/eli/ligj/2012/04/26/48/e16d165b-487f-4be9-9735-39b512894e01;q=per%20mbrojtjen%20e%20te%20dhenave%20personale>;
Law No. 9887, dated 10 March 2008 "On Personal Data Protection" <https://qbz.gov.al/eli/ligj/2008/03/10/9887/41ed4e3c-3dde-4028-9755-11887c48b7f6;q=per%20mbrojtjen%20e%20te%20dhenave%20personale>.
15 Law on copyright and other rights related to it as of 31 March 2016 <https://qbz.gov.al/eli/ligj/2016/03/31/35/e78a22e9-d479-430f-bae6-c7a3dbcd33f0;q=per%20mbrojtjen%20e%20te%20dhenave%20personale>.
16 Ministry of Defence, Cyber Protection Strategy 2018-2020. <http://www.mbrojtja.gov.al/images/PDF/2017/Strategjia_Mbrojtjen_Kibernetike_2018_2020.pdf>.

— 'The crosscutting strategy Albania's digital agenda 2015-2020' – Decision of the Council of Ministers.[17]

2.4. Please include reference to any policy papers and/or proposals.

As mentioned on paragraph one of question number two there is a proposal currently being reviewed in the Parliament of Albania, a proposal which has faced a lot of criticism and has been turned back to the Parliament by the President as explained above. The Parliament is currently waiting to receive the Venice Commission opinion requested by the Monitoring Committee of the Parliamentary Assembly of the Council of Europe. Regarding that, the Council of Europe's Commissioner for Human Rights released the below-quoted statement.

'I am deeply concerned to learn that this week the Albanian Parliament pursued the examination of two draft laws, known as the 'Anti-Defamation Package'. These laws are in need of urgent improvement. Several provisions are indeed not compatible with international and European human rights standards which protect freedom of expression and freedom of the media.

I am particularly concerned that discretionary powers given to regulatory bodies, the possibility to impose excessive fines and to block media websites without a court order, as well as the introduction of state regulation of online media, may deal a strong blow to freedom of expression and media freedom in the country. It is of the utmost importance to ensure that the Internet remains an open and public forum and that self-regulation by the media, including online media, prevails.

I therefore urge members of the Parliament of Albania to review the current drafts and bring them in line with the case law of the European Court of Human Rights and Council of Europe standards.'[18]

17 Decision of the Council of Ministers, No. 284, dated 1 May 2015, accessed on 18 January 2020.

18 Statement by the Council of Europe Commissioner for Human Rights, Commissioner urges Albania's Parliament to review bills which restrict freedom of expression <https://www.coe.int/en/web/commissioner/-/commissioner-urges-albania-s-parliament-to-review-bills-which-restrict-freedom-of-expression> accessed on 28 January 2020.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

3.1. Differences in treatment between in civil and criminal law

While the content considered unlawful in civil law and criminal law differs as explained below, what we can find a similarity on, is the lack of specific regulations regarding the blocking, filtering and taking down of internet content. Although that remains true up until this date, it does not mean that content cannot be taken down or blocked using the current regulations. The court may use these regulations as a base to do that in the context of consequences resolution in it is decision.

3.2. Blocking and taking down otherwise legal content

The Albanian Penal Code contains a number of provisions that penalise criminal offences performed through the Internet; however, it does not provide legal regulations to the blocking or filtering of illegal Internet content.[19]

The Albanian Penal Code,[20] as amended, provides that intentional dissemination of statements, and any other pieces of information, with the knowledge that they are false, affect a person's honour and dignity, shall constitute criminal misdemeanour, and is punished by a fine of 50 thousand to 1 million five hundred thousand ALL. Where that act is committed in public, to the detriment of several persons, or more than once, it shall be punished by a fine of 50 thousand to 3 million ALL.

Intentional insult[21] of a person shall constitute a criminal misdemeanour, and is punished by a fine of fifty thousand to one million ALL. The same act, when committed in public, to the detriment of several persons, or more than once, constitutes a criminal misdemeanour and shall be punished by a fine of 50 thousand to 3 million ALL.

Another provision in the Albanian Penal Code concerns the sharing of materials of racist or xenophobic content through electronic systems. These actions constitute criminal misdemeanour and are punished by fine or deprivation of liberty for up to two years.

19 Swiss Institute of Comparative Law, Comparative study on blocking and takedown of illegal internet content, page 6, paragraph 7.
20 Article 120 of the Albanian Penal Code, as amended.
21 Article 119 of the Albanian Penal Code, as amended.

Similar to the Penal Code regarding the issue, the Albanian Civil Codes provides regulations concerning compensation for non-pecuniary damage but offers no specific regulation regarding the blocking or filtering of illegal content online.

Article 647/a - *The manner and criteria for determining civil liability and the extent of non-pecuniary damage* - of the Albanian Civil Code, as amended, provides that compensation for non-pecuniary damage for the infringement of a person's honour, personality or reputation, aims at restoring the infringed right in proportion to the damage suffered and is determined on the basis of the circumstances of the case. In determining civil liability and the extent of non-pecuniary damage, the court also takes into account:

- The manner, form and timing of the dissemination of the statements or the performance of the acts;
- The extent to which the author of the statements complies with the rules of professional ethics;
- Forms and degree of guilt;
- Whether the statements have correctly quoted or referred to the statements of a third person;
- Whether the statements are false, especially in the case of reputation infringement;
- Whether the statements relate to matters of the injured person's private life and their relationship to a public interest;
- Whether the statements constitute opinions or statements that contain only trivial factual inaccuracies;
- Whether the statements relate to matters of public interest, or to persons in public office or candidates for election;
- Acting to prevent or reduce the extent of the harm, such as making a false disclaimer, and any other measures taken by the author of the allegedly defamatory personality, reputation or reputation;
- Whether the author of the false statements has derived benefits from their propagation and the extent of such benefit;
- The fact that indemnification can significantly aggravate the financial situation of the person causing the damage.

According to the law 'On protection of personal data', as amended, lawful processing of personal data shall be respected and the rights and fundamental freedoms shall be ensured, in particular, the right to privacy. Therefore, in a situation where the lawful processing of personal data prejudices rights and fundamental freedoms and in particular, the right to privacy, the Commissioner

for Personal Data Protection has the right to order the blocking, deletion, destruction or suspension of the unlawful processing of personal data.

Following the law 'On copyright and other rights related to it', as amended, if an infringement of copyright does not constitute a criminal offence, it may still constitute an administrative infringement, which is punishable by a fine. This law punishes harmful or illegal actions that infringe intellectual property rights, but it does not regulate the issues of internet content when certain actions performed through the internet infringe intellectual property rights.

The 'Cyber Defence Strategy 2018-2020' by the Ministry of Defence document addressed the plan of action for the protection from cyber-attacks and the security of information and communication in the field of military defence in the Republic of Albania. While it expresses the so-called 'Security Challenges' that originate from four sources among others, the internet, mobile devices, social networks and portals, it does not clarify the measures the Ministry of Defence will take to tackle these security challenges.[22]

The crosscutting strategy Albania's digital agenda 2015-2020 set out by a Decision of the Council of Ministers addressed the functions of the plan of action in the context of a secure internet to carry out several activities for online protection of children's rights, through the signing of the Code of Conduct by which the entrepreneurs engage in providing technical tools for filtering and parental consulting provisions for the protection of children and young people from illegal content and harmful electronic communications.[23]

3.2.1. Safeguards to ensure a balance between censoring and freedom of expression

The Constitution of Albania, in Articles 22 and 23 provides for freedom of speech, freedom to receive and impart information, and freedom of the press. However, there are reports that the government and businesses influence and pressure the media.[24] There are no government restrictions on access to the Internet or reports that the government monitors e-mail or Internet chat rooms without appropriate legal authority.

22 Paragraph 6 and 7, page 9 of reference no. 12.

23 Minister of State for Innovation and Public Administration, Cross-Cutting Strategy "Digital Agenda of Albania 2015-2020", Page 15 and 17 <http://ogp.gov.al/uploads/2018/12/Strategjia_Axhenda_Dixhitale_e_Shqiperise_2015-2020.pdf> Accessed on January 2020.

24 Albania - Country Reports on Human Rights Practices for 2018, Bureau of Democracy, Human Rights and Labour, accessed on 14 February 2020.

The Constitution of Albania prohibits censorship; yet, the law may require authorisation for radio and TV broadcasting. Hate speech is forbidden. The Constitution also grants citizens the right to access to information: every citizen has the right, in accordance with the law, to acquire information on the activities of state bodies and persons exercising public functions. The Authority for Electronic and Postal Communications decreed on 15 October 2018, that 44 media web portals had 72 hours to obtain a tax identification number and publish it on their web pages or the government would shut them down.[25] The list included several investigative news sites. At year's end, the government had not shut down noncompliant portals.[26]

3.3. Judicial review of takedown cases

Article 617 of the Albanian Civil Code, as amended, provides that, when it is certified that a person is liable towards another person, because he has published incorrect, incomplete and fraudulent data, the court upon request of the damaged person, obliges the other person to publish a confutation, in the way that it would consider it appropriate. The court can order the publication of a confutation even when it is proven that the publication of data is not illegal and done by fault, if their author had no knowledge of the incorrect or incomplete character of this data. However, the current legal framework in force, does not provide any *specific* regulation with regard to blocking, filtering or take down of illegal content published on the internet.

In practice, subjects affected by an online post, may require the court, and the latter may decide the respondent party is obliged take down the online publication, in accordance with Article 625 of the Albanian Civil Code, which provides as follows:

'A person suffering non-pecuniary damage shall be entitled to compensation when:

- has suffered damage to his health, physical or mental integrity;
- his honour, personality or reputation has been violated;
- the right of name has been violated;
- respect for private life has been violated;
- the memory of a dead person has been violated. In this case, the spouse of the deceased person or his relatives up to the second degree may claim non-pecuniary damage compensation.'

25 ibid, page 10.
26 ibid, page 10.

Although the law does not explicitly provide for the submission of such a claim by the entity, the reason for this legal vacuum may be the failure to update the Albanian Civil Code with the situations and violations arising from the use of electronic media.

In addition to classifying the taking down of online content as part of the compensation of the individual suffering non - pecuniary damage, the removal/deletion of online content may also be required in practice as a precautionary measure until the final decision of the court. However, considering the position of the courts on a case-by-case analysis, this requirement is seen as disproportionate and is not normally approved by the court, as it may interfere with freedom of expression of the respondent party.

According to the amended Audio-Visual Media Law, the interested entity or the penalized entity may file an appeal with the AMA Board within 30 days of the date of publication or notification of the Appeals Commission (AC) decision, as provided by this law. Appealing against the AC decision does not suspend the execution of the decision. The AMA Board reviews the appeal and announces the decision no later than 10 days. The AMA Board's decision can be appealed in the Administrative Court of Tirana (first instance).[27]

3.4. Compliance with the case law of the European Court of Human Rights

As the Republic of Albania has ratified the European Convention on Human Rights (ECHR) with Law no. 8137 dated 31 July 1996, the Constitution of Albania is in full compliance with the provisions of the ECHR. Also, Law 91/2019, provides that any provision of these amendments is interpreted and applied in accordance with the principles of the ECHR and Fundamental Freedoms, as it applies to the legal practices of the European Court of Human Rights.[28]

Referring to some of the most iconic case law of the European Court of Human Rights,[29] limitations on freedom of expression foreseen in Article 10(2) of the

---

27 Article 132, paragraph 6 of the Law 91/2019, dated 18 December 2019, On some additions and amendments on the Law No. 97/2013 on Audio Visual Media in the Republic of Albania.

28 Article 4/1, paragraph 2 of the Law 91/2019, dated 18.12.2019, "On some additions and amendments on the Law No. 97/2013 on Audio Visual Media in the Republic of Albania". Accessed on 1 February 2020.

29 *Delfi AS v. Estonia* [GC], no. 64569/09, 16 June 2015; *Ashby Donald and Others v. France*, no. 36769/08, § 34, 10 January 2013; *Handyside v. the United Kingdom*, 7 December 1976; *Aleksey Ovchinnikov v. Russia*, no. 24061/04, § 51, 16 December 2010.

ECHR are interpreted strictly.[30] Interference by States in the exercise of that freedom is possible, provided it is:

- 'necessary in a democratic society', that is to say, according to the Court's case law, it must correspond to
- a 'pressing social need',
- be proportionate to the legitimate aim pursued within the meaning of the second paragraph of Article 10, and
- justified by judicial decisions that give relevant and sufficient reasoning.[31]

Whilst the national authorities have a certain margin of appreciation, it is not unlimited as it goes hand in hand with the Court's supervision.[32]

As mentioned above, referring to the Albanian courts case law, there are very few cases where the court has ordered blocking or taking down of online content/publications. In view of this approach, it can be concluded that Albanian courts consider the deletion of online publications a disproportionate measure and an unnecessary restriction on freedom of expression.

3.5. Case law

The plaintiff Tirana Municipality alleged that the respondent Mr. A.D, in the capacity of a member of the Tirana Municipality Council and at the same time Chairman of the group of advisers of the political party 'Socialist Party of Albania', made several statements according to which the Municipality of Tirana and the Mayor of Tirana it is alleged that funds for decorating the holiday of independence have been disbursed directly to private companies owned by the mayor's family members. These statements, which were transmitted by audio and visual messages, were addressed to the Municipality of Tirana and the citizen Mr. L.B, in the exercise of his function and powers as Mayor of Tirana, alluding to corruption and abuse of these funds.

On 1 December 2011 the press and audio – visual chronicles of informative editions of popular television channels, published several statements given by respondent Mr. A.D, being thus, widely spread in the public opinion. The first (full) statement was published on the Socialist Party's official website www.ps.al, as well as broadcast in all local and national media as well as in the print media.

---

30 Council of Europe/European Court of Human Rights, on Internet case law, updated June 2011 <https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf>p. 17, accessed on 2 February 2020.

31 ibid, page 17.

32 ibid, page 17.

According to the plaintiff, the statements of the respondent in the function of a member of the Tirana City Council and the head of the group of advisers of the Socialist Party are unlawful and do not constitute a factual truth. According to the applicant, these statements seriously affect both the Mayor and the Municipality of Tirana in his personality, having a direct impact on the community and public opinion, and for such circumstances the plaintiff has addressed the Tirana Judicial District Court with a lawsuit.

3.5.1. The Decision of Tirana District Court (First Instance)

Tirana Judicial District Court, by Decision no. 8802, dated 01 October 2012 decided that there was an obligation of the respondent Mr A.D to publish a confutation on the matter.

The obligation of the respondent Mr. A.D to pay in favour of the plaintiff the amount of ALL 1 million) as compensation for the non- pecuniary damage caused to the plaintiff.

The Tirana District Court argues, *inter alia,* that Albanian civil Code has created and guaranteed a special protection for the honour and personality of the person, protecting individuals from the unlawful conduct that infringes them.

The Court notes that non-pecuniary damage, as provided by Article 625/1/ a of the Albanian Civil Code, is one of the types of non - contractual damage. The concept of non - contractual damage is provided by Articles 608 and 609 of the Civil Cod. In this particular judgment, the court observes that unlawful conduct consists in the use of words or expressions that interfere with the honour and personality of a particular person. The plaintiff alleged that he was caused a non-pecuniary damage as a result of using expressions that infringe on his honour and personality in the statements of the respondent cited above.

3.5.2. Tirana Court of Appeal Decision

The Tirana Court of Appeal, by Decision no. 940, dated 19 April 2013, decided to enact of Decision no. 8802, dated 1 October 2012 of the Tirana Judicial District Court, regarding the publication of a confutation of the statements of the respondent Mr. A.D.

Amending this decision, forcing respondent Mr. A.D to pay in favour of the plaintiff the sum of ALL 200,000 (two hundred thousand) for the non-pecuniary damage caused.

Later on, in the High Court of Albania the plaintiff Tirana Municipality filed Claim no. 1285, dated 29 March 2018, with object waiver of the right to sue, according to which the plaintiff party, Tirana Municipality, based on Article 201

/ a of the Code of Civil Procedure states that it waives the right to sue completely, seeking the dismissal of the lawsuit.

This particular case reflects the approach of the Albanian Courts and Applicants, which are still reluctant to decide or request the court to decide (in the case of the damaged individuals) the blocking, filtering or taking down of illegal internet content, as there is no specific regulation with this regard.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

4.1. Code of Ethics for Journalists

The self-regulation of blocking and taking down internet content is still in a rudimentary phase. There is no record on any kind of self-regulation act of the online media in Albania by the private sector itself. However, there is a non-governmental organization of journalists, named the Albanian Media Council (Këshilli Shqiptar i Medias) which is created with the purpose to promote self-regulation among the community, as a mean to re-establish trust and maintain media's credibility with the Albanian public.[33] This organisation, conscious about the gap of media self-regulation, is trying to fill it by adopting a Code of Ethics for Journalists (Kodi i Etikës së Gazetarit) which contains several provisions regarding the truthfulness of information, copyright protection, and other principles which should lead a journalists' profession and activity. The seventh part of this Code, named 'Responsibility after the publication', provides the following provisions:

- The publisher and the editor are responsible for publishing news, articles, letters to the editor, comments and responses in the media website, including the case where the name of the author is removed or set as a nickname.
- The media and editorial board must agree and publish clearly defined conditions for the selection and publication of comments by the public. The media should monitor and review these comments and take steps to ensure that the conditions of publication are respected.
- The media has the right to add a 'note' to the comments and responses, or even decide not to publish them at all, unless it has previously promised to do so. The editorial board reserves the right to edit or shorten letters to the editor, or comments, provided that the editing does not change their meaning. If the media outlet decides to publish a letter

[33] The Albanian Media Council, <http://kshm.al/en/albanian-media-council/> accessed on 13 February 2020.

to the editor or comment, it must do so within a reasonable time between their submission for publication and the time of publication.

— Before publishing a comment, or a letter to the editor, containing serious allegations against a third party, the editor or the editorial board should investigate whether there are grounds for such allegations. The accused should also be given the opportunity to respond.

— It would not be realistic to expect all comments to be read, edited or rejected before publication. However, the editorial board or editors may delete or remove inadmissible comments from the publication when they are abusive, hate speech, or deemed to contain malicious and unfounded claims. Where there is a complaint that a comment contains serious allegations or insults to a third party, the editorial board and editors should investigate whether there is any basis for such allegations and, if not, the comment should be removed from publication.

The seventh part of the abovementioned Code contains the only cases when blocking or taking down internet content are mentioned explicitly in this act.

4.2. Grievance redressal mechanisms

The norms set in the Code of Ethics for Journalists shall be considered as soft law, as even though the Council has the right to receive complaints and give decisions, this process has a moral value, and it can be implemented only voluntarily by the journalists. The Council's Board does not give orders through their decisions, but just state if there is any infringement and give certain recommendations, e.g. to take down the online article, as it happened in the case of *A.T. vs Shqiptarja.com*.[34] This recommendation was respected by the online portal that initiated this news, but the rest of the online portals which had copied the news have ignored it, and this article can still be found online in multiple websites. This case reflects another problem in the Albanian online news area: copyright infringement. This is a common breach of law in the online Albanian news portals. Many news articles are copied from the source, and republished by different portals. This phenomenon is obvious only by doing a simple search on the internet.

However, even though this is a practiced mechanism in Albania, it is not necessarily efficient. The Council admits itself that the Code of Ethics is never applied when the wrongdoing should be repaired.[35]

[34] The case of A.T vs Shqiptarja.com <http://kshm.al/2019/03/21/alice-taylor-kunder-shqiptarja-com/> accessed on 13 February 2020.

[35] History of the Albanian Media Council <http://kshm.al/en/about-us/history/> accessed on 15 February 2020.

4.3. The most frequent recommendations made by the Albanian Media Council

The Albanian Media Council had published the breaches of the Code of Ethics monthly until May 2018,[36] and for unknown reasons these updates were interrupted. Such reports of the Council showed the concrete online news articles containing certain infringements made by the journalists, and the recommendations made by the Council. The most frequent recommendations include:

- Journalists should carefully follow the rules of the Albanian language and avoid using foreign words whenever possible.
- The media should clearly distinguish comment from assumption and facts.
- In reporting and especially in comments or controversy, journalists are obliged to respect the ethics of public speaking and the culture of dialogue.
- Journalists must respect the honour and reputation of individuals who become objects of their professional interest.
- Journalists should never call attention to personal or private aspects unless they are important.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

The legal framework setting out rules with regard to personal data protection within the territory of the Republic of Albania is the Law No. 9887, dated 10 March 2008 'On Personal Data Protection'[37], as amended. Current law on personal data protection does not explicitly provide for the 'Right to be Forgotten' or the 'Right to Delete' as postulated and interpreted by Article 17 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 'On the protection of natural persons with regard to the processing of personal data and on the free movement of such data' which repealed Directive 95/46/EC (hereinafter the GDPR).[38]

Nevertheless, the above mentioned law provides for data subjects to request for their data to be blocked, readjusted or removed when such data are not accurate,

36 Observations by the Albanian Media Council <http://kshm.al/category/vezhgime/> accessed on 19 February 2020.

37 Law No. 9887, dated 10 March 2008, On Personal Data Protection.

38 Law No. 9887, dated 10 March 2008, On Personal Data Protection.

true, comprehensive or the processing or collection of personal data has not occurred pursuant to the law.

Article 13 of the Law 'On Personal Data Protection' sets out as following:

'The data subject is entitled to obtain from the controller the blocking, rectification or removal of data, free of charge, when his/her data are not accurate, true, comprehensive or the data are not processed and collected in accordance with the provisions of this law.

The controller, within 30 days from the day of receipt of the data subject's claim, should inform him/her on the lawfulness of data processing, on the completion or incompletion of blocking, rectification or removal.

If the controller does not block, readjust or remove the data as requested, the data subject is entitled to submit a complaint to the Commissioner.'

According to Article 3(5) of the Personal Data Protection Law, the 'controller' refers to a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the aims and means of the processing of personal data, in compliance with the relevant laws and bylaws, and is responsible for fulfilling obligations as set out by this law.

In that context, data subjects can request to have personal information removed by a controller if their data is unlawfully being processed. Anyhow, this cannot be interpreted as the right to be forgotten nor the right to delete as provided for by the new Regulation on GDPR. Article 13 of our national law aims at establishing the right of data subjects to restrict or delete their data processing, while the new Regulation rules a new outlook on how this right can be exercised under GDPR as well as extends its application to already published data of a subject.

The new Regulation 2016/679 clarifies and broadens the territorial scope of its legal effects by taking into account both the place of establishment of the data controller and the place of residence of the data subject.[39] In that light, the new regulation will be applicable to the processing of personal data by controllers and processors that are located in the EU countries, regardless of whether or not the processing is carried out in these countries. This means that no matter where the processor of the data is located, within or outside the European Union when offering services to European consumers, they must apply and meet

[39] Joaquín Muñoz Rodríguez, Pablo Uslé Presmanes, Ana Rocha, Ana Festas Henriques, Derek Stinson and Paula Enriquez, Territorial Scope of Regulation (EU) no. 2016/679 <https://www.lexology.com/library/detail.aspx?g=d4dbdb56-5f8b-4421-a428-7e674b5af423> accessed on 25 July 2020.

GDPR requirements, meaning that the Regulation will extend its effects within the Republic of Albania when specific requirements are met (i.e. the processing of data toward a EU citizen is occurring).

Furthermore, in the framework of Stabilization and Association Agreement between the Republic of Albania and EU, Article 70 of SAA states that 'the parties recognise the importance of the approximation of Albania's existing legislation to that of the Community and of its effective implementation. Albania shall endeavour to ensure that its existing laws and future legislation shall be gradually made compatible with the Community acquis. Albania shall ensure that existing and future legislation shall be properly implemented and enforced'. In this light, the Albanian Information and Personal Data Protection Commissioner has incorporated into the Strategy 'On Information and Personal Data Protection' of 2018-2020 the approximation of the national legal framework with the GDPR.[40] According to above mentioned strategy, the transposition of the Regulation is foreseen to be completed by the end of 2020. The alignment of national legal framework is necessary not only due to the relationship between Albanian businesses and foreign investors/entities - which means that companies are now more subject to the application of new provisions of the GDPR but also to respect the right to privacy of the Albanian citizens.

Since the Albanian legislation has not incorporated the provisions of the new Regulation on GDPR yet, there is no jurisprudence of our national courts and administrative authorities with regard to that issue. Also, there is no practice of the Commissioner for data protection regarding the Article 13 of the above mentioned law.

6. How does your country regulate the liability of internet intermediaries?

6.1. The regulation

The issue with regard to internet intermediaries is regulated by Law No.10128, dated 11 May 2009 On electronic trade,[41] as amended. The judicial regime (Article 15, 16 and 17) provided by the above mentioned law is based on the lack of responsibilities towards the Information Service Provider, if the service is limited solely to simple broadcasting (mere conduit), temporary storage of the

40 Strategy 2018-2020: Protection of Personal Data, page 18 <https://www.idp.al/wpcontent/uploads/2018/02/Strategjia_per_te_Drejten_e_Informimit_dhe_Mbrojtjen_e_te_Dhenave_Personale.pdf>.

41 Law for Electronic Trade of 11 May 2009 <http://qbz.gov.al/eli/ligj/2009/05/11/10128>.

information (caching), or hosting activity and if certain conditions postulated in Article 15, 16 and 17 are met.

More precisely Article 15 (Mere Conduct) of the Law sets out that:

'1. When the Information Service Provider consists only in transmitting a communication network of information provided by the service receiver, or in providing access to a communication network, the service provider shall not be responsible for the broadcasted information, if the service provider: (a) does not initiate broadcasting (b) does not opt or modify the content of the broadcasted information (c) do not choose the receiver of the transmission.

2. Actions of broadcasting and providing access, in compliance with point 1 of the Article, shall include the automatic, immediate and temporary storage of the broadcasted information solely for conveyance of the transmission to a communication network, by ensuring the storage of information for as long as needed for broadcasting.'

Article 16 (Caching) of the Law sets out that:

'During the transmission of information to the communications network, the service provider providing broadcasting of information shall not be responsible for the temporary, intermediate and automatic storage, performed solely to increase the efficiency of transmission of information to other service receivers, as requested by them, if the Provider: (a) does not modify the information (b) fulfils/acts in accordance with the conditions of access to information (c) fulfils/acts in accordance with the rules for information update, in a specified, well-known and broadly-used manner (d) does not interfere with the legitimate use of known - technology and widely-used by the electronic communications industry to obtain data on the use of information (e) operates promptly to remove or deactivate access to stored information, as soon as it comes to its knowledge that the information on its initial source of transmission has been removed from the network, the access to it has been disabled/deactivated or the responsible authorities have ordered its removal or deactivation.'

Article 17 (Hosting) of the Law sets out the following:

'1.When an Information Service Provider consists on storage of information provided by the receiver of the service, the ISP shall not be responsible for the information stored based on a request of the service receiver, if the service provider: (a) is not unaware or could not be aware of the unlawful activity of the receiver or the content of the information and as per concerns with regard to damages, is not aware of facts or circumstances from which the unlawful activity or information derives (b) as soon as it acquires such information, acts promptly

to remove or deactivate the access to the information. 2. Point 1 of this article shall not apply when the receiver of the service acts on behalf or under the control of the service provider.'

Nevertheless, Article 19 of the Law on Electronic Trade provides for the possibility of termination or forestalling an infringement, and more specifically the Articles provides for: 'Regardless of the postulations on the provisions of this law, especially in Articles 15, 16, 17 and 18, the Service Provider is obliged to terminate or forestall an infringement, if the court or authorities in charge request so, in compliance with the legislation into force.'

Furthermore, according to the Law No. 9918, dated 19 May 2008 On electronic communication,[42] as amended, the Authority for Electronic Communications and Postal is the regulatory body in the field of electronic communication and it is responsible for the implementation and monitoring and regulating the activity of subjects of electronic communication network and subjects providing services on electronic communications (hereinafter electronic communications providers). In that context, according to Article 14 and 15 of the law, AECP registers the electronic communication providers and by authorising commencement of their activity it also requires compliance with restrictions on illegal or detrimental content as provided for by the law in force (among other conditions). Also, referring to Annex E of the Regulation no.47, dated 26 October 2017 On enforcement of the General Authorisation regime, Point 9 provides for the legal steps to discontinue and block the broadcasting of illegal or detrimental content. After the AECP receives a request from the authority in charge for restricting the broadcast of unlawful or detrimental content, addresses the issue to the internet intermediary requesting the discontinuance and blocking of the broadcasting of an unlawful/detrimental content (See Article 19 of the Law on Electronic Trade as above mentioned as well). The internet intermediary is obliged to act immediately and to fulfil the solicit.

As an illustration of the above mentioned laws, we shall give an overview of an case related to blocking of access to a satiric online pg. www.kryeministria.com (in English: www.primeministry.com). According to AKEP (in English: the Agency for Electronic and Postal Communication), a request to block the access to this page was filed by the AKCESK (in English: the National Authority for electronic Certification and Cybersecurity). Upon such request, based on Article 15/1 (e) of the Law No. 9918, dated 19 May 2008 On Electronic

42 Law No. 9918, dated 19 May 2008 On electronic communication <https://akep.al/wpcontent/uploads/images/stories/AKEP/legjislacioni/ligji9918ndryshuar-versioni-publikim-web190313.pdf> accessed on 30 of February 2020.

Communication in the Republic of Albania which sets out that: 'In the general authorisation, AKEP sets out conditions regarding compliance with restrictions related to unlawful or damaging content, according to relevant legal regulations in force.' Also, the AKEP points out that based on Article 9/1 (e) and Article 9 of the Annex E of Regulation No. 47, dated 26 October 2017 on Endorsement of General Authorisation Regime where it is determined that: '1. Transmissions determined as having unlawful or damaging content on the basis of a decision taken by the competent authorities as defined in the relevant legislation, restrictions shall apply. 2. The undertaking/entity providing the network and/or the electronic communications services shall have the legal obligation to take the appropriate legal and technical measures to implement the required restriction. 3. AKEP, upon the request of the relevant competent authority to restrict broadcasting of unlawful or damaging content, shall address to the undertaking/the entity providing the network and/or public electronic communications services, to discontinue and block the broadcasting of this content. 4. Upon receipt of the request by the AKEP to restrict the broadcasting of unlawful or damaging content, the undertaker is obliged to act immediately to disconnect and block the broadcasting.'

Based on the above mentioned legal reasoning, the AKEP forwarded the request to cease the access to this page to the Electronic Communication Undertakers residing in the territory of the Republic of Albania. Furthermore, the AKEP brought forward in his arguments that the competent institution to block the access to a page is not AKEP, but other competent authorities (as provided for by relevant laws), and in the current occasion, it was the AKCESK the competent authority that requested such blocking.

AKCESK, based the request on the following arguments: Upon efforts to communicate with the source of the page to obtain detailed information about the page, the institution was unable to do so as no public data of the online page was provided. Also, after ascertaining the usage of the emblem of the prime ministry, violating Article 8 of the Law on shape and size of the national flag, content of the national anthem, shape and size of the emblem of the Republic of Albania as well as the manner to use them, which allows only institutions of central power. Based on the above mentioned reasons, the AKCESK on the grounds of Article 10 of the Law No. 2/2017 on Cybersecurity and Decision of the Council of Ministers No. 141, dated 22 February 2017, point 4.21 which states that: 'The Authority establishes, administrates and maintains the unique online system, for the publication of online pages containing unlawful content, as follows […] (a) […] (b) […]' concluded that this page may constitute a jeopardy for the blocking of another official portal (www.shqiperiaqeduam.al)

and addressed the issue to the AKEP for the latter to verify the page and to notify the ISP to take imminent measures to block the access to the page.'

Currently, this page cannot be accessed within the territory of the Republic of Albania.

Having mentioned the applicable law regarding the liability of internet intermediaries we can conclude that when certain conditions are met, the Information Service Providers (internet intermediaries) shall not be held responsible for any (unlawful) activity, storage of information (as requested by the receiver of the information or in terms of efficiency) and as a result is not liable for blocking and taking down content.

In the occasion that the ISPs exceed their role as simple broadcasters then they will not fall under the protection provided by the law on electronic trade (exclusion from liability). And, if the competent authorities request for disconnection or blocking of the access to an unlawful page/portal, the ISP are bound to respect such request.

On the other hand, the Parliament of the Republic of Albania has recently adopted the (draft) Law No. 91/2019 On some amendments and additions to Law No. 97/2013 On Audiovisual Media in the Republic of Albania, as amended. Following the newly amendments, the concept of the right to response indicates the opportunity/possibility for a subject whose reputation is directly violated by untruthful or inaccurate facts and information published under the Electronic Publications Service Provider (hereinafter the EPSP), to lodge a written request with the EPSP putting forward his arguments and facts in support of his claims for violation of reputation. Upon such request, the EPSP within 48h from receipt of the claim shall determine on whether to exercise or reject the right to response and if decides in favour of the subject concerned, the response (of the person subject to an alleged violation of reputation) will be published in the same page the content is released. Nevertheless, the EPSP is not obliged to publish the response if: (i) the subject concerned has not a legitimate interest to deliver a response (ii) the response inappropriately surpasses the degree to which facts concerned are proclaimed (iii) the response is not limited only to factual information or involves content with regard to a prosecution. Furthermore, Article 132 of the Law describes the measures to be taken by the responsible authority (AAM) in the occasion of contents published from the EPSP. The provision entitles the Authority of Audiovisual Media to:

— order for erasure or prevention to access the content which according to the criminal legislation in effect is alleged to constitute a criminal offense

as follows: (a) children pornography (b) acts for terrorist purposes c) infringement of national security;

— obliges the EPSP to put a 'pop-up' announcement in the website/portal's domain, consisting of information about the decisions undertaken by the decision-makers of the AAM.

The decision will be taken upon a request of the National Authority for electronic certification and cybersecurity or other competent authorities.

Law does not incorporate steps on how measures will be implemented, nevertheless, it guides the responsible authority to implement measures which should have the least impact on freedom to expression and such measures shall be into force for a specified period of time.

Jurisprudence of our national courts play an increasingly important role with regard to settling various issues that are not directly provided by specific provisions. In this context, the national Courts have developed a significant jurisprudence aiming to solve disputes arising from publications (fake or not) and the two above-mentioned mechanisms are widely used to regulate judicial consequences. In their analyses, the Courts endeavour to find a fair balance between freedom of expression and the right to privacy. The following cases implicate common politicians and immunity issues while exercising their duties, freedom of expression, the balance between freedom of expression and insulting or libelling by using the power of duty.

The Supreme Court of the Republic of Albania in one of the cases, on Decision No. 28 dated 25 April 2016, displays an allegation with regard to libelling. The complainant (Mr. H) accuses Mr. F.N for libelling during the election campaign of 2015. Referring to the statements made publicly by Mr.F.N during the electoral meeting in a city in Albania, the complainant pretends violation of honour and dignity. He also argues that such publicly false statements have been broadcasted in local news editions and published in the official page on Facebook of Democratic Party. The defendant, according to the complainant, was aware of spreading inaccurate information and it has consequently damaged the image of Mr. H has affected his honour, dignity and personality and such statements are made deliberately to cause the loss of faith of citizens toward the complainant.

In a nutshell, the Penal College of the Supreme Court decided that the statement during the electoral meeting did not constitute a criminal offence due to the lack of meeting two components: the subjective and objective aspect of a criminal offence. The statements made by Mr. F.N fall under the protection provided by Article 10 of the Convention on Human Rights (including the freedom of

opinion, the freedom to participate in or give information, or opinion without intervention of state authorities and without taking into account state limitations/borders) and Article 22 of the Albanian Constitution, which guarantees the freedom of expression. Taking into consideration relevant cases of the EHRC, the Supreme Court states that Article 10 extends its application to all the manners of expression which manifest opinions, ideas, information, regardless of their content or the way of broadcasting,

In another argument, the Court states that such declared information does not objectively violate the dignity, honour and the perception of the public toward the complainant. Even if the information would be true, it would not be deemed as to cause damages to his image. Furthermore, the court takes into account the intention of the speech during the election campaign of 2015, it comes to the conclusion that the intention of Mr.F.N was not to violate the name or the personality of the complainant but to inform the public on the inadequacy of the previous governance, to address his concerns and to collect votes in the framework of an electoral race. The defendant cannot be held responsible for libelling if the disseminated affirmations were true or if the defendant had reasons to believe in the veracity of such affirmations.

In conclusion, the Court sets out that the speech and statements of the defendant are concluded in the framework of the electoral race, to inform the public as well as in the framework of the freedom of expression while exercising his duty and since the complainant did not bring any evidence to provide his claims, such statements shall be deemed to be completed bona fide.

Referring to another case submitted with the District Court of Tirana, entailing the Prime Minister F.N (at the time the dispute was being administered) and others against the company Time and Our Time Newspaper – on grounds of insulting and libelling the Prime Minister requested for compensation due to violation of his honour and personality, as a result of a publication made by the Our Time Newspaper. The Court decided that the expressions used in the published article extend the limit of being new of an informative nature or of a criticism aiming to give information to the public about politician leaders with regard to their duty or their social life. Such expressions constitute a violation of the reputation (honour and personality). As a result, the Court decided in favour of the plaintiffs and recorded a fine amounting at 2 million, as a compensation for violating the right to reputation.

In the following case, the District Court of Tirana among the compensation required from the respondent to publish a counterblast as well, resolving the judicial consequences based on the Civil Code. An ex-deputy of the Democratic

Party (Mrs. J.T) has been indicted for libelling by Prime Minister E.R after she made a statement on her official Facebook page that gambling had been quadrupled during Rama's governance. The District Court of Tirana issued the following decision: 'Obligation of the Respondent, J.T to pay to the Claimant E.R in compensation for the non-pecuniary damage caused by her declaration on the Facebook page dated 25 October 2018 the amount of ALL 300 thousand.' Furthermore, the Court compel J.T to publish a counterblast on her Facebook page related to the declaration made on 25 October 2018, within seven days from the issuance of the Decision.

Despite the aforementioned laws and provisions, there is not any law regulating specific measures for blocking and taking down content on online media or any rule regarding the right to online expression, nevertheless, the Articles of the Civil Code and Criminal Code are deemed to cover the absence of specific provisions establishing steps with regard to blocking and taking down content.

6.2. Safeguards

The current legal framework follows the principle of self-regulation of media and aims at creating an environment which enables individuals to access and share information and to fully enjoy the freedom of expression online. In this context, the national legal framework promotes the freedom of expression of online media and regulates the activity of the latter to the extent needed to balance the freedom of expression and the right to privacy and the protection of one's reputation.

Article 22 of the Constitution of the Republic of Albania sets out as follows:

- Freedom of expression is guaranteed.
- Freedom of the press, radio and television is guaranteed,
- Prior censorship of communication means is prohibited

Referring to Article 11 of the Law No. 9887, dated 10 March 2008 On Personal Data Protection, as amended provides for the exclusion from obligations with regard to protection of personal data, processing of personal data, processing of sensitive data, international transferring of data, the obligation to inform the subject on the processing of data, and the obligation of the controller to notify the Commissioner on the processing of data. Such exclusion is foreseen to be performed for journalism, literary and artistic purposes.

Article 4/1 of the (draft) Law On Audiovisual Media in the Republic of Albania (not published with the Center for Official Publications) postulates that 'the provision of the law shall not be interpreted in a way that censures or restricts the right to freedom of expression. The law is interpreted and implemented in

compliance with the principles of the European Convention for Protection of Human Rights and Fundamental Freedoms, as applicable in legal practices of the European Court of Human Right.' In addition, the law (Article 132/5) provides that if the Authority of Audiovisual Media undertakes measures regarding the erasure of the content or prevention of access to the content which constitutes a criminal offence, such implemented measures should represent the least impact on the right to freedom of expression and in compliance with the principles of necessity and proportionality.

On the other hand, as mentioned above the jurisprudence of our national Court has developed and extended the protection provided by provisions of the Civil Code and the Criminal Code when certain conditions are met. In terms of online publications, subjects are obliged to not libel, insult or not to publish fraudulent information otherwise they may be subject to a litigation. Also, subjects are entitled to request information to the Agency for Electronic and Postal Communication with regard to the author of a damaging publication (violating the image of a subject, the reputation, honour etc.) for them to be able to initiate a civil process with the Court (as mentioned above).

Among constitutional protection of freedom of expression and other provisions provided by relevant laws, the Republic of Albania has in addition ratified international agreements such as: Universal Declaration of Human Rights of United Nations, European Convention for protection of Human Rights and Fundamental Rights (and its Protocols), International Convention on Civil, Political Rights (and its Protocols). The above mentioned Agreements form an integral part of the national legislation therefore the freedom of expression can be protected and interpreted in accordance with their provisions and no less protection can be provided by the national legislation.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and takedown, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Bearing in mind that Albania is a state party and has ratified the European Convention on Human Rights; it also has certain obligations arising from the Stabilization and Association Agreement with the European Union, - inter alia, the obligation to adapt its legislation with the European Union Regulations and Directives, - the legal framework related to the protection of online freedom of

expression, liability of internet intermediaries and the right to be forgotten will continue to be adapted with these instruments.

Our democracy is still fragile and needs further improvements with regard to balancing certain rights and freedoms. The Republic of Albania ever since 1990 has continued its endeavour to protect freedom of expression and on the other side to take steps to safeguard the dignity and the honour of individuals. Referring to all the actions undertaken as to date from the competent institutions, and more precisely: (1) amendments and additions of law on Audio-visual Media (2) Adoption of Strategy On Information and Personal Data Protection of 2018-2020 regarding the approximation of the national legal framework with the new GDPR, indicate further interventions in issues that regulate the blocking and taking down content and the right to be forgotten. Also, in terms of implementation of EU regulations and adhering of Stabilization and Association Agreement, the national legislation is expected to be amended and to reflect the EU regulations.

On the other hand, incorporation of provisions with regard to online content blocking and takedown is necessary, although the current framework provides for some steps to be taken in case of unlawful contents (as mentioned in previous questions). In conclusion, we believe that our legal framework shall be enriched in new amendments of the current laws, as well as adoption of new provisions, which will display clearer legal steps regarding online content blocking and takedown and the right to be forgotten. As per liability of internet intermediaries the Parliament of the Republic of Albania has not initiated any draft-law aiming at amending the current law, nevertheless, following the adoption of the new EU GDPR and new amendments of the law on audio-visual media, certain regulations of the law on electronic trade (or the electronic communication) may be needed.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in the online environment? If not, what needs to be done to reach such balance?

As mentioned above, the legal framework regarding online content blocking and takedown, liability of internet intermediaries and the right to be forgotten is still outdated. the law does not explicitly provide for the submission of such a claim by the entity, the reason for this legal vacuum may be the failure to update the Albanian Civil Code with the situations and violations arising from the use of

electronic media. When the Albanian Civil Code was adopted, publications were made only in newspapers/print media, and the articles after publication could not be deleted as they were published and distributed hard copy, and consequently the only efficient measure that could be taken was to publish a retraction of the news in the same medium.

Today, electronic media offers the possibility of deleting and blocking illegal content, therefore, there must be an initiative to change and adapt the civil code in terms of fraudulent publication, with technological innovations and the situations arising from the use of electronic mass media. Of course, this measure can only be requested and taken in cases where the court finds that the restriction of freedom of expression fulfils the proportionality criterion and other criteria set by the ECtHR.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

When discussing the freedom of expression in Albania it is important to keep in mind its history regarding fundamental human rights. After an authoritarian regime lasting around half a century, where the freedom of expression was not protected, Albania ratified the European Convention of Human Rights only in 1996 and adopted the Constitution by referendum in 1998. This background is important to understand Albania's policy-making regarding the freedom of expression in the last 25 years.

There has been an obvious overall goal to be as strict as possible when it comes to limiting the freedom of expression online. We can see that by the almost complete lack of specific regulations of online media until 2019. If that course of policy-making regarding freedom of expression online will continue the same or change, is something to be observed in the future months, especially after the opinion of the Venice Commission gets released.

Despite the careful policy-making to keep the limiting of freedom of expression online as close to none, that does not mean that other rights were completely disregarded. Regulations spread on different laws in Albania clearly show no tolerance for some types of activities or content relating to terrorism, xenophobia, child pornography and cybercrime.

The area where the lack of specific regulations on online content has caused more issues to arise would be defamation. The Albanian Civil Code regulations

regarding defamation have shown to not be effective. A large number of the subjects affected by false news decide to not even take the matter into the court because of the lengthy complicated process and obvious convenience issues.

Internal self-regulation of Albanian online media has also been lacking, resulting in more problems regarding the spread of false information. An initiative from a non-profit organisation Albanian Media Council aiming to contribute for a more ethical and professional media has not been effective in tackling the issue.[43] Beside its activity on calling out ethical breaches in online media the NGO has shown to not be effective and has brought no significant results in improving the situation.

Considering what was said above, some may come to the conclusion that sometimes protecting the freedom of expression online might have come at the cost of other rights such as the right to a private life, but that statement needs to be read with a grain of criticism since there is not yet any relevant case law to have proved a breach in the right to a private life because of content published online.

The balance between the freedom of expression and other fundamental rights is a pretty delicate one and at times the scale may seem to lean a little bit more to the side of the freedom of expression online in Albania. This might change with the new controversial regulations proposed just months ago and the Venice Commission opinion on the draft law currently being reviewed in Albanian Parliament will surely help the last-mentioned find a way to keep the scale as even as possible.

10. How do you rank the access to freedom of expression online in your country?

In a scale from 1 to 5, with one being the lowest access and five the highest, we rank the freedom with 2. In first sight, Albania might deserve a maximal evaluation, as in practice it may seem that the online media is free to write whatever they like, without being censored about anything.

However, this has had certain negative results. Practically, the media is as free, as it is harmful to other parties. Copyright infringements and fake news have become national customs and there are no efficient mechanisms to stop it. Self-regulation is almost non-existent, and even when it exists, it is not enforced. The worst that can happen to the freedom of expression is to pollute facts and

[43] About the Albanian Media Council <http://kshm.al/en/about-us/> accessed on 10 January 2020.

information with disinformation and lies because essentially everything is then regarded by the public (the news consumer) as lies, and this right loses its core meaning. Such conclusions can be made simply by taking a look at the Albanian Media Council's cases.

According to the government, such situations have brought a need for special laws to guide the online media in the right path and to correct such problems. These special laws, informally called the Anti-defamation Package (Paketa Antishpifje),[44] have caused broad controversy in the country. In the time when the Authority of Audiovisual Media was the organ that supervised the media activity, the new laws added a second institution with such competences, the Authority of Electronic and Postal Communications. This reform was thought to supress the online media, as it would be supervised now by two different institutions. The president of Albania approved a presidential decree institutionalising his approach against these changes. [45] In the presidential decree, it was said that concerns about spreading fake news, or the negative impact of misinformation, should be addressed in such a way that any legal means of protection against these phenomena will in no way endanger, imbalance, or create the risk of misuse of these tools to violate the right to information, freedom of expression and of the media or even freedom of economic activity, rights that enjoy special protection under the Constitution and international acts. However, the notes made in the presidential decree were disregarded by the parliament.

On the other hand, not only these laws may fail to correct the current unlawful situation, but may have a negative impact, as they put the government in a very superior position towards the media. Even though that one of the amendments states that interpretations that censor or limit the right to freedom of speech cannot be made,[46] it is possible that it would remain an unenforced disposition.

So, the Albanian legal framework on online media is now in a vicious circle, where if the laws are unenforced, this would show a lack of control by the state; and if they are enforced, they could breach the freedom of expression.

---

44 This package is made of two laws, respectively: Law No. 91/2019 and Law No. 92/2019.

45 Presidential Decree No.11414, dated 11 January 2020, On the return of law, No. 92/2019 On some additions and changes on the law, No.9918 dated 19 May 2008 On the electronic communications in the Republic of Albania, amended.

46 Article 6 of Law no. 91/2019 On several amendments and additions of law, no. 97/2013 on audiovisual media in the Republic of Albania, amended.

11. How do you overall assess the legal situation in your country regarding internet censorship? Incorporate the answers you have given to the previous questions and the main findings.

As previously stated, after 40 years of communism the Republic of Albania plunged itself to democratic system in 1991. Following the alteration of the system, the country faced various rights and freedoms, which at that moment were unknown, undiscovered and completely challenging. Since then, Albania has established a tradition of self-regulation, or as less restriction to freedom of expression as possible. The Constitution of the Republic of Albania, in Article 22 guarantees the freedom of expression and also the freedom of press, radio and television. It prohibits prior censorship to means of communications, which shall include the internet. However, the regulation of the online sphere is rather liberal regarding its content. The law sanctions only content on genocide or crimes against humanity, as well as provocation of ethnic, religious or other hate, and the Chief Prosecutor has the competences and obligations to react accordingly, including collecting and accessing all relevant content. The regulation of the technical aspects is rather different. It requires any citizen to make a formal request in order to acquire a permit for a website by the Authority on Electronic and Postal Communication (AKEP), which is responsible for the technical regulation of online media.

Another law addressing issues regarding the freedom of expression in Albania is Law No. 97/2013 'On the audiovisual media in the Republic of Albania' and (draft) Law No. 91/2019 'On some amendments and additions to Law No. 97/2013 On Audiovisual Media in the Republic of Albania', aiming, according to the authorities, at fighting against defamation. Article 4(1) of the (draft) Law postulates that 'the provision of the law shall not be interpreted in a way that censures or restricts the right to freedom of expression, and also provides for steps to be taken in the occasion of violation of reputation by publishing untruthful or inaccurate facts (see Question 6 for further details).

In overall, although there is no judicial internet censorship, in practice the situation is quite different (referring to Reports published by relevant NGOs and Albanian journalist's opinions). The adoption of the (draft) Law No. 97/2013 has gotten a negative feedback from some journalists and a number of non-profit organisations that work on the field of human rights and has been considered controversial by many. If passed by Parliament, the proposed amendments would empower a state administrative body (the Audio Visual Media Authority) to regulate content published by online media. The draft bills seek to tighten the control over online media, as the Complaints Council, which

is part of the Audio Visual Media Authority, could increase censorship by ordering the removal of online content on grounds of protecting the citizens' dignity and privacy. Several international organisations joined Albanian civil society and independent media in calling the government to withdraw these bills.[47] Currently, an opinion of the Venice Commission concerning this law is requested by the Monitoring Committee of the Parliamentary Assembly of the Council of Europe.

Furthermore, the Albanian Media Council (AMC), an NGO comprised of journalists and media professionals, has accused Prime Minister Edi Rama of exploiting the emergency situation caused by the earthquake of 26 November 2019 and illegally shutting down online media by allegedly ordering the AKEP (Electronic and Postal Communications Authority) to block online news portals, including joqalbania.com. On 1 December 2019, the AMC posted a Declaration of Concern About the Government Attitude Towards Media, stating that the authorities 'cannot prohibit citizens or portals from denouncing the mismanagement of the situation (where it exists) and, furthermore, cannot block an entire portal for a single publication.' According to Reporter Al, Prime Minister Rama has 'repeatedly expressed dissatisfaction with the media' when faced with difficult questions on the government's ability to effectively manage the aftermath of the earthquake. According to journalist Gjergj Erebara, Prime Minister Rama has used social media platforms on a number of occasions to put pressure on online portals, threatening closure. He tweeted on 28 November 2019: 'This is the final warning for portals and information channels that under the conditions and within the legal framework of an Emergency Situation, I will be obliged to forcibly intervene with their closure to end this dramatic phase, if they continue with fake news that spread panic!' Another video message was shared on Facebook on 3 December 2019 where Prime Minister Rama addressed the general public, asking them to avoid watching the news on television and implored not to follow the online portals stating that the 'so-called sources of information' create a 'foul-smell of gloom and insecurity and confusion'. While the AMC appeals to the media to show restraint in reporting unverified news, it also calls for the Government 'not to copycat the notorious Erdogan case that used the post-coup situation to attack, arrest, shut down and hit critical media; to silence independent opinions; and to install the dictatorship of thought.'

---

47 Council of Europe, Media Freedom Alerts (search for Albania in 2019) <https://www.coe.int/en/web/media-freedom/allalerts?p_p_id=sojdashboard_WAR_coesojportlet&p_p_lifecycle=0&p_p_col_id=column-4&p_p_col_count=1&_sojdashboard_WAR_coesojportlet_keywords=&_sojdashboard_WAR_coesojportlet_selectedStringFilters=year.2019&_sojdashboard_WAR_coesojportlet_selectedCategories=11709474> accessed 26 July 2020.

Having said that, we can conclude that in terms of legal framework, the freedom of online expression, as to date, has developed and is protected by certain provisions, trying to find a balance between the right to (online) expression and the right to privacy (or other related rights) by aiming to protect the honour/reputation of individuals in one hand and to not narrow the freedom to express opinion or to give/receive information. Whatsoever, referring to what happens in Albania in practice, we can conclude that further steps to protect the freedom of expression are necessary. In a democratic state, journalists are entitled to report situations that aim to give rise to important issues occurring within the country. As every other right, there must be limitation where appropriate, but such limitations should be made in accordance with the EU regulations and with the least intervention of the State.[48]

[48] Council of Europe, Prime Minister Pressures Online Portals and Information Channels <https://go.coe.int/sA7yn> accessed 30 July 2020.

Table of legislation

Provision in Albanian language	**Corresponding translation in English**
Kushtetuta e Republikës së Shqipërisë, Neni 22: 1. Liria e shprehjes është e garantuar. 2. Liria e shtypit, e radios dhe e televizionit është e garantuar. 3. Censura paraprake e mjeteve të komunikimit ndalohet. 4. Ligji mund të kërkojë dhënien e autorizimit për funksionimin e stacioneve të radios ose të televizionit.	The Constitution of Republic of Albania, Article 22: 1. Freedom of expression is guaranteed. 2. Freedom of the press, radio and television is guaranteed. 3. Prior censorship of means of communication is prohibited. 4. The law may require authorization to be granted for the operation of radio or television stations.
Kushtetuta e Republikës së Shqipërisë, Neni 23: 1. E drejta e informimit është e garantuar. 2. Kushdo ka të drejtë, në përputhje me ligjin, të marrë informacion për veprimtarinë e organeve shtetërore, si dhe të personave që ushtrojnë funksione shtetërore. 3. Kujtdo i jepet mundësia të ndjekë mbledhjet e organeve të zgjedhura kolektive.	The Constitution of Republic of Albania, Article 23: 1. The right to information is guaranteed. 2. Everyone has the right, in compliance with law, to obtain information about the activity of state organs, and of persons who exercise state functions. 3. Everyone is given the possibility to attend meetings of elected collective organs.
Ligji Nr.8410 Datë 30.9.1998 "Për radion dhe televizionin publik dhe privat në Republikën e Shqipërisë", neni 35, paragrafi 2: Në programet radiotelevizive nuk lejohet censura.	Law No.8410 Date 30.9.1998 "On the public and private radio and television in the Republic of Albania", Article 35, paragraph 2: Censorship is not allowed in the radio and television programs.
Ligji Nr.7756 Datë 11.10.1993 "Për Shtypin", Neni 1: Shtypi është i lirë. Liria e shtypit mbrohet me ligj. Shtypi kufizohet vetëm nëpërmjet dispozitave të kushtetutës dhe këtij ligji. Ndalohet marrja e çdo mase tjetër që prek lirinë e shtypit.	Law No.7756 Date 11.10.1993 "On the Press", Article 1: The press is free. Freedom of the press is protected by law. The press is limited only by the provisions of the constitution and this law. It is prohibited to take any other measure affecting freedom of the press.

Ndalohet themelimi i organizatave profesionale të shtypit me anëtarësi të detyruar dhe krijimi i gjykatave special për shtypin me pushtet diktues mbi të.	The establishment of professional press organizations with mandatory membership and the establishment of special press courts with dictatorial powers is prohibited.

Bibliography

English titles

Legislation

Constitution of the Republic of Albania

Law No. 8410 Date 30 September 1998 "On the public and private radio and television in the Republic of Albania"

Law No. 7756 Date 11 October 1993 "On the Press"

Presidential Decree No. 11414 Date 11 January 2020 "On the return of law No.92/2019 "On some additions and changes on the law No. 9918 date 19 May 2008 "On the electronic communications in the Republic of Albania", amended"

Code of Ethics for Journalists

Reports

Online Media Landscape in Albania: Online media survey, Albanian Media Institute, Tirana 2018

Albanian titles

Legislation

Kushtetuta e Republikës së Shqipërisë

Ligji Nr.8410 Datë 30.9.1998 "Për radion dhe televizionin publik dhe privat në Republikën e Shqipërisë"

Ligji Nr.7756 Datë 11.10.1993 "Për Shtypin"

Dekret Presidencial Nr.11414 Datë 11.01.2020 "Për kthimin e ligjit Nr.92/2019 "Për disa shtesa dhe ndryshime në ligjin Nr.9918 datë 19.5.2008 "Për komunikimet elektronike në Republikën e Shqipërisë", i ndryshuar

Peizazhi i Medias Online në Shqipëri: Anketë me median online, Instituti Shqiptar i Medias, Tiranë 2018

ELSA Armenia

Contributors

National Coordinator

Arpine Arakelyan

National Researchers

Anita Grigoryan

Ani Hunanyan

Lilit Harutyunyan

Lilit Hayrapetyan

Luiza Meliksetyan

National Linguistic Editor

Leyli Tadevosyan

National Academic Supervisor

Arpine Hovhannisyan

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

The protection of freedom of expression has gone through considerable changes in Armenia after the destruction of the Soviet Union.

As the freedom of expression is one of the most essential rights for every human being and for every democratic state the Republic of Armenia provides vital provisions concerning this right.

The Constitution of the Republic of Armenia has the highest legal power. According to the paragraph 1 of Article 42 of the Constitution of the Republic of Armenia everyone shall have the right to freely express their opinion. This right shall include freedom to hold own opinion, as well as to seek, receive and disseminate information and ideas through any media, without the interference of State or local self-government bodies and regardless of State frontiers.[49]

The freedom of media, TV and radio broadcasting and other means of communication is guaranteed as well. According to the Constitution of the RA the freedom of the press, radio, television and other means of information shall be guaranteed. The State shall guarantee the activities of independent public television and radio offering diversity of informational, educational, cultural and entertainment programmes.[50]

The paragraph 3 of Article 42 of the Constitution of the RA states that the freedom of expression of an opinion may be restricted only by law, for the purpose of State security, protecting public order, health and morals or the honour and good reputation of others and other basic rights and freedoms thereof.

First of all, freedom of expression is protected and guaranteed at the constitutional level in Armenia. Everyone can hold an opinion and express it and search, receive and impart information and ideas regardless of frontiers.

The Constitution of the RA also provides the right to information. Everyone shall have the right to receive information and get familiar with documents relating to the activities of State and local self-government bodies and officials.[51] According to the paragraph 2 of Article 51 of the Constitution the restrictions on the right to receive information might be imposed only by law, for the

49 Paragraph 1 of the Article 42 of the Constitution of the Republic of Armenia dated 6 December 2015.
50 Paragraph 2 of the Article 42 of the Constitution of the Republic of Armenia dated 6 December 2015.
51 Paragraph 1 of the Article 51 of the Constitution of the Republic of Armenia dated 6 December 2015.

purpose of protecting public interests or basic rights and freedoms of others. The procedure for receiving information, as well as the grounds for liability of officials for concealing information or for unjustified refusal of providing information thereby shall be prescribed by law.[52]

According to the Constitution of the Republic of Armenia everyone shall have the freedom of literary, artistic, scientific and technical creation.[53] The Constitution states that everyone has the freedom of literary, scientific and technical work, hence the State does not have the jurisdiction to censor these spheres.

The above-mentioned articles indicate that censorship is banned in Armenia. There is no definition for censorship in the national legislation, but there are some essential provisions in legal acts that indicate that the censorship is banned in the RA.

Censorship is a form of state control over the content and dissemination of information, publishing, music and literary works, radio and television broadcasting, websites and portals, as well as personal communication. The aim of censorship is to prevent and ban the dissemination of such information and ideas that are undesirable to the authorities.

Although censorship is prohibited at the legislative level, we cannot deny the existence of hidden censorship, especially for mass media. This can be done through funds, coercion, sponsorship and other means.

Everyone can freely express their opinion on the internet, but there is not any legal act which provides this right. The Republic of Armenia does not have a legal act that regulates issues related to the censorship and freedom of expression on the internet. There are no special oversight bodies in the Republic of Armenia that will supervise the protection of freedom of expression and prohibition of censorship. It is important to mention that there is a Committee to Protect Freedom of Expression (CPFE) in the RA. It is a non-profit journalistic organisation. The main activities of this Committee are monitoring the state of freedom of expression in Armenia, identifying and responding to violations of the rights of journalists and the media and publishing periodic reports based on the received data. According to this Committee's report, the third quarter of 2019 has been marked by an unprecedented stream of new lawsuits with the involvement of journalists and the media. Within the monitoring period, thirty-three cases had proceedings in different courts. Out of these cases thirty were

52 Paragraph 3 of the Article 51 of the Constitution of the Republic of Armenia dated 6 December 2015.
53 Article 43 of the Constitution of the Republic of Armenia dated 6 December 2015.

based on insult and slander under Article 1087.1 of the RA Civil Code, two cases were on violations of the right to receive and disseminate information and one was a lawsuit of a media outlet against a politician.[54]

There are some legal acts that guarantee freedom of expression and ban censorship. One of them is the legal act On Mass Media.[55] The implementers of media activity and journalists shall operate freely in compliance with the principles of equality, legitimacy, freedom of speech (expression) and pluralism.[56] This Law states that the following is prohibited:

- Censorship,
- To compel the implementer of media activity or a journalist to disseminate or refrain from the dissemination of information,
- Interfering with the legitimate professional activities of a journalist,
- Discrimination in public circulation of appliances and materials necessary for dissemination of information, restriction of a person's right to exploit media products of their choice, including those issued and disseminated in other countries.[57]

As Armenia does not have a legal act that regulates issues related to the censorship and freedom of expression on the internet, the paragraph 3 of Article 4 of the Law on 'Mass Media' can be used in an analogous way and refers to the internet content as well.

The right to freedom of expression is not absolute, especially in the case of dissemination of materials in the scope of conducting journalistic activity. It is forbidden to disseminate information or speech that is classified as secret or criminally punishable by law, as well as the dissemination of the information that violates the inviolability of personal life. In addition, the dissemination of information obtained by video recording is prohibited, if it has been obtained without warning the person about recording, and that person has expected that they are out of the performer's view, is not audible to them and has taken sufficient measures to do, except when the measures taken to get out of view or not to be heard were clearly insufficient. The above-mentioned information is allowed to be disseminated, if it is necessary for the protection of the public

54 Third Quarter Report by CPFE on Situation with Freedom of Expression and Violations of Rights of Journalists and Media in Armenia (2019) <https://khosq.am/en/reports/third-quarter-report-by-cpfe-on-situation-with-freedom-of-expression-and-violations-of-rights-of-journalists-and-media-in-armenia-2019/> accessed 4 February 2020.

55 Law No. 14 dated 8 February 2004 On Mass Media.

56 Paragraph 1 of Article 4 of Law No. 14 dated 8 February 2004 On Mass Media.

57 Paragraph 3 of Article 4 of Law No. 14 dated 8 February 2004 On Mass Media.

interest. The European Court of Human Rights has referred to the notion of public interest. According to ECtHR, although the public has a right to be informed, and this is an essential right in a democratic society which, in certain special circumstances, can even extend to aspects of the private life of public figures, articles aimed solely at satisfying the curiosity of a particular readership regarding the details of a person's private life, however well known that person might be, cannot be deemed to contribute to any debate of general interest to society.[58] This means that it is important to have balance between freedom of expression and inviolability of private life.

The case law of the Republic of Armenia refers to the notion of public interest as well. The paragraph 3 of Article 7 of the RA legal act 'On freedom of information' provides that if it is not otherwise foreseen by the Constitution and/or the Law, information holder at least once a year publicise the following information related to their activity and or changes to it:

- Activities and services provided (to be provided) to public;
- Budget;
- Forms for written enquiries and the instructions for filling those in;
- Lists of personnel, as well as name, last name, education, profession, position, salary rate, business phone numbers and e-mails of officers:
- Recruitment procedures and vacancies;
- Influence on environment;
- Public events' program;
- Procedures, day, time and place for accepting citizens;
- Policy of cost creation and costs in the sphere of work and services;
- List of held information and the procedures of providing it;
- Statistical and complete data on inquiries received, including grounds for refusal to provide information;
- Sources of elaboration or obtainment of information mentioned in this clause;
- Information on person entitled to clarify the information defined in this clause.

58 Couderc and Hachette Filipacchi Associés v France App no 40454/07 (ECHR, 10 November 2015).

According to the Constitutional Court of the RA the latter is the minimum information that should be available to everyone as information of public interest. However, this does not limit the scope of information of public interest. Every person, including an organisation, should have the opportunity to demand or become acquainted with the information under the control of state or local self-government bodies, if the provision of such information does not violate the protection of public interests or the rights and freedoms of others. Moreover, the Law On freedom of information provides for the scope of information, which in any case cannot be a basis for restricting the provision of information based on a violation of the public interest.[59] According to the Law On freedom of information information request cannot be declined, if:

- It concerns urgent cases threatening public security and health, as well as natural disasters (including officially forecasted ones) and their consequences;
- It presents the overall economic situation of the Republic of Armenia, as well as the real situation in the spheres of nature and environment protection, health, education, agriculture, trade and culture;
- If the decline of the information request will have a negative influence on the implementation of State programs of the Republic of Armenia directed to socio-economic, scientific, spiritual and cultural development.[60]

The Court of Cassation of the RA states that the superior public interest is directly related to the public's right to be informed. When assessing the superior public interest, it is important to answer these questions whether the information was significantly needed, or the public followed up on the dissemination of that information and waited for its further publication. The media is responsible for disseminating information on issues of public interest, including the dissemination of ideas. This function (duty) of the mass media is combined with the right of the public to receive information.[61]

A person has a right to demand the implementer of media activity to refute factual inaccuracies in the information disseminated by the implementer of media activity if the latter does not prove the truth of those facts. The demand

59 Constitutional Court of the Republic of Armenia, Decision of 23 February 2016 No. SDV-1256, pages 13-14, available in Armenian, <http://www.concourt.am/armenian/decisions/common/2016/pdf/sdv-1256.pdf>, accessed 26 May 2020.

60 Paragraph 3 of Article 8 of Law No.11 dated 15 November 2003 On freedom of information.

61 Cassation Court of the Republic of Armenia, Decision of 27 April 2012, No. LD/0749/02/10, section 4, point B.

for refutation has to be presented within a one-month period following the day of publication of the information subject to refutation.[62] The mentioned one month is a limitation period. The paragraph 5 of Article 8 of the Law On Mass Media states that along with refutation, a person has the right to demand publishing of a response. The implementer of media activities may choose to accompany or not the publishing of the response along with refutation. By publication of the response the right to refutation is considered fulfilled.[63]

A demand for a refutation and/or a response shall be denied if it is:

— Anonymous;

— Contradicts a court decision that entered in a legal force.[64]

The demand for refutation or response may also be denied if

— The term stipulated by part 1 of this article has not been complied with;

— The demand is related to such information that has been disseminated with a reference to a public speech, official documents of State bodies, other media product or work of authorship and the original source has not disseminated a refutation.[65]

If an implementer of media activities refuses to publish the refutation or the response, or infringes the terms and procedures of their dissemination as provided by this law, the person whose rights are violated has a right to file a lawsuit demanding to disseminate the refutation or response.[66]

These regulations allow to protect the rights violated as a result of the abuse of the right to freedom of expression.

The legal act On the libraries and the activity of libraries also refers to the prohibition of censorship in the Republic of Armenia. Restricting access to library collections for censorship is prohibited.[67] It can be concluded from this, that there is no censorship in the sphere of creativity, accessibility of literature and scientific materials in the RA.

One of the important acts against censorship is the legal act On television and radio, which regulates the activities of television and radio companies. The paragraph 1 of Article 4 of this legal act provides a statement that guarantees the

62 The paragraph 1 of Article 8 of Law No. 14 dated 8 February 2004 On Mass Media.
63 The paragraph 5 of Article 8 of Law No. 14 dated 8 February 2004 On Mass Media.
64 Paragraph 7 of Article 8 of Law No. 14 dated 8 February 2004 On Mass Media.
65 Paragraph 8 of Article 8 of Law No. 14 dated 8 February 2004 On Mass Media.
66 Paragraph 9 of Article 8 of Law No. 14 dated 8 February 2004 On Mass Media.
67 Paragraph 9 of Article 11 of Law No. 90 dated 18 May 2012 On the libraries and the activity of libraries.

right to choose freely, produce and distribute television and radio programs. Censorship of television and radio programs is prohibited. Everyone has the right to free reception of television and radio programs and additional information, including satellite, cable networks, free or paid, both by decoding means and by open networks of television and radio broadcasting.[68] The State shall create the necessary conditions and take measures for the reception of programs of the Public Television and Radio Company (at least one TV channel and one Radio Station) in the Republic of Armenia.[69] Interference in the activities of television and radio companies by State authorities, government officials, parties, NGOs and other legal and natural person is also prohibited. Interference by State authorities in these activities is only possible in cases provided by the legislation of the Republic of Armenia.

Although the right to freedom of expression is the cornerstone of democratic states, it is, nevertheless, subject to restrictions in some cases. It is forbidden to use television and radio broadcasting for the following:

- For propaganda to seize power by force, to forcibly change the constitutional order of the Republic of Armenia;
- To incite national, racial and religious hostility or separations;
- To preach war;
- To propagate acts that are prohibited by law;
- To distribute pornography, abuse scenes or cruelty;
- For the purpose of broadcasting programs that contain or propagate acts of violence and cruelty.[70]

The paragraph 2 of Article 22 of the legal act On television and radio states that erotic TV shows and movies containing horror and outrageous violence, as well as programs that may have negative impact on juvenile mental and physical development, and education, with the exception of subscribed broadcasting, may be aired from 24:00-6:00 am.

As the right to freedom of expression includes the freedom to seek, receive and impart information and ideas, there is also a need to regulate these issues at the legislative level. In this regard, the following two laws are applicable in the

68 Paragraph 2 of Article 4 of Law No. 97 dated 18 November 2000 On television and radio.
69 Paragraph 3 of Article 4 of Law No. 97 dated 18 November 2000 On television and radio.
70 Paragraph 1 of Article 22 of Law No. 97 dated 18 November 2000 On television and radio.

Republic of Armenia: the legal act On freedom of information and the Law On protection of personal data.

The paragraph 1 of the Article 1 of the RA legal act On freedom of information states that this legal act defines the jurisdiction of the holders of information, as well as the procedure, forms and conditions for receiving information. Every person has the right to have access to the information they sought to and/or to request the information holder and to receive that information according to the law.[71] The Article 3 of the legal act On freedom of information defines the notion of the information holder: State and local self-government bodies with information, State institutions, organisations financed from budgets, as well as public organisations and their officials.

Freedom of information is based on a number of principles: unified ordering for registration, classification or preservation of information, protection of the freedom to seek and receive information, ensuring access to information and publicity. The holder of information must promptly publish or otherwise make available to the public the information, which may prevent the threats to public security, public order, public health or morals, threats to the rights and freedom of others, environment or property. The Law also regulates the cases, when the right to information may be restricted. The holder of information rejects the disclosure of information, if it contains State, official, banking, commercial secrets, violates the privacy of correspondence, telephone conversations, mail, telegrams and other communication, contains preliminary investigation data, discloses data requiring restriction of access to professional activity (medical, notarial, legal secrets), violates copyright and/or associated rights.[72]

If the information holder refuses to provide the information required by the written request, they shall notify the applicant in written form within five days, stating the ground for refusal (the relevant norm of the law), as well as the procedure for its appeal.[73] Refusal to provide information may be appealed to an authorised public administration body or court.[74]

As it was mentioned above, the second law concerning the balance between the right to information and the right to personal privacy is the RA Law On protection of personal data. It regulates the procedure and conditions for the processing and control of personal data by public administration or local self-government bodies, State or community agencies or organisations, legal or

71 Paragraph 1 of Article 6 of Law No. 11 dated 15 November 2003 On freedom of information.
72 Paragraph 1 of Article 8 of Law No. 11 dated 15 November 2003 On freedom of information.
73 Paragraph 3 of Article 11 of Law No. 11 dated 15 November 2003 On freedom of information.
74 Paragraph 4 of Article 11 of Law No. 11 dated 15 November 2003 On freedom of information.

natural persons. According to the Law On protection of personal data the processing of personal data implies any activity or group of activities, irrespective of the form and method of implementation (including automated, any technical means or without them), that is related to the collection or preservation or entry, coordination, organisation or related to the usage or transformation, to recovery, correction, blocking, destroying of personal data or performing other actions.[75] Restrictions on the processing of personal data set by this Law are not applicable exclusively to personal data processed for journalistic, literary purposes. Personal data are processed for legitimate and specific purposes and cannot be used for any other purposes without the consent of the data subject.[76] Data processing should have legitimate purpose, and the means to achieve it should be appropriate, necessary and moderate. During the processing of personal data, the developer must use encryption measures for the protection of information systems containing personal data from accidental loss, unlawful access to information systems, illegal use, recording, destruction, transformation, blocking, copying, dissemination, sharing, etc.[77] Without the consent of the data subject, the developer may transfer the personal data to third parties or provide access to the data if it is provided by law and has a sufficient level of protection.

The Criminal Code of the Republic of Armenia is also concerned with the right to freedom of expression and contains provisions on hate speech and prescribes punishment for the latter. The paragraph 1 of Article 226 of the Criminal Code of the RA provides punishment for acts of national, racial or religious hostility, racial superiority or degrading national dignity. The aggravating circumstances for this crime are:

- The commission of these acts, whether publicly or through the use of mass media;
- The commission of these acts by using violence or threat of violence;
- The use of official position or commission of these acts by an organised group.[78]

The Criminal Code of Armenia provides punishment for the public calls for violence, public justification or propaganda of such violence based on gender, race, skin colour, ethnic or social origin, genetic background, language, religion, worldview, political or other views, national minority, property status, birth,

75 Paragraph 1 of Article 3 point 2 of Law No. 49 dated 1 July 2015 On protection of personal data.
76 Paragraph 2 of the Article 4 of Law No. 49 dated 1 July 2015 On protection of personal data.
77 Paragraph 2 of the Article 19 of Law No. 49 dated 1 July 2015 On protection of personal data.
78 Paragraph 2 of Article 226 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.

disability, age or other personal or social circumstances[79] if there are no features of the crimes such as failure to actively comply with a lawful request by a government official during mass riots or calls for violence against persons,[80] acts of national, racial or religious hostility, racial superiority or degrading national dignity,[81] public calls for terrorism, terrorist financing and international terrorism, publicly justifying or propagating the commission of these crimes,[82] public calls to seize power, violate territorial integrity or forcibly overthrow constitutional order,[83] public calls for aggressive war,[84] the denial, mitigation, approval or justification of genocide and other crimes against peace and human security.[85] The aggravating circumstances provided by the Criminal Code for this provision are the following:

- the commission of these acts by a group of persons with prior consent or by an organised group;
- the commission of these acts by using the official position.[86]

This provision was adopted by the National Assembly of the RA on 15 April 2020.

Article 144 of the Criminal Code stipulates the responsibility for disseminating, collecting or retaining personal or family secret information in public speeches, publicly displayed works or media without their consent, unless it is provided by law.

The Criminal Code restricts the right to freedom of expression by providing responsibility for violating the privacy of a person's correspondence, telephone conversations, mail, telegraph or other communications.[87]

Restrictions on freedom of expression are also stated in Article 263 of the Criminal Code of Armenia. Paragraph 1 of this Article provides liability for disseminating, advertising, sale or preparing pornographic materials or objects, including printed publications, film and video materials, images, if there is no evidence of the characteristics of human trafficking or exploitation, trafficking or exploitation of a child or a person deprived of the opportunity to understand the nature and significance of their actions. Paragraph 2 of this Article provides

79 Paragraph 1 of Article 226.2 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
80 paragraph 4 of Article 225 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
81 Article 226 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
82 Paragraph Article 226.1 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
83 Article 301 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
84 Article 385 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
85 Article 397.1 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
86 Paragraph 2 Article 226.2 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
87 Article 146 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.

punishments for introducing child pornography through a computer system or maintaining child pornography on a computer system or computer data storage system.[88]

The abuse of the right to freedom of expression can also damage one's reputation, dignity or business reputation. RA Civil Code provides protection and compensation of one's honour and dignity in case of insult and/or defamation.

Insult is a public expression made to defame honour, dignity or business reputation through speech, image, voice, sign or otherwise. Public expression and its content in a given situation may not be considered offensive, if they are based on accurate facts (except for disabilities) or are caused by a predominant public interest.[89]

Defamation is the public submission of a statement of fact that is untrue and distorts one's honour, dignity or business reputation.[90] Paragraph 5 of the Article 1087.1 of the RA Civil Code stipulates that public disclosure of factual data is not considered defamatory:

- If it is a statement made in a pre-trial or judicial proceeding or evidence presented by a trial participant;
- With its content it is connected with a predominant public interest and if a person, who submitted statement of facts publicly, proves that they have taken reasonable steps to establish its truthfulness and reasonableness, as well as have presented the data in a balanced and conscientious way;
- It is from defamed person's or their representative's public speech or response or document.

A person shall be exempt from liability for insult or defamation if the factual information expressed or presented by them is the literary or conscientious reproductions of the information disseminated by a media or another person's public speech, official documents, other media or copyrighted work and by disseminating it a reference was made to the source (author) of the information.[91] In case of insult, a person can apply to court by demanding to apologise publicly. The form of apology is determined by court. If the insult is found in a media outlet, a person may demand to publish the whole or the part judgement of the

88 The paragraph 2 of Article 263 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
89 Paragraph 2 of Article 1087.1 of Law No. 239 dated 1 January 1999, the Civil Code of the RA.
90 Paragraph 3 of Article 1087.1 of Law No. 239 dated 1 January 1999, the Civil Code of the RA.
91 Paragraph 6 of Article 1087.1 of Law No.239 dated 1 January 1999, the Civil Code of the RA.

court through the media. The method and volume of the publication is determined by court.[92]

As the RA legislation does not have special regulations for the cases of defamation or insult on the internet, the above-mentioned provisions are applied in an analogous way for these cases. In case of insult, the person may require paying compensation in the amount of 1000-fold of the defined minimum salary.[93]

In case of a defamation the person may require, through judicial procedure, the application of one or several of the following measures:

— Where the defamation appeared in the information disseminated by an entity carrying out media activities, public refutation of factual data considered as defamation and/or publication of its response with regard thereto. The form of refutation and the response shall be approved by the court, guided by the Law of the Republic of Armenia On Mass media.

— Paying compensation in the amount of 2000-fold of the defined minimum salary.[94]

If the source (author) of the information is not known while insulting or defaming, or the media, exercising its right not to disclose the source, does not disclose the author's name, then the one, who has offended or the slanderer, shall be liable for the compensation, and if the defamation or insult is disseminated by the media, the one who performs media activity shall be liable for the compensation.[95]

In conclusion, we can say that the Republic of Armenia guarantees the right to freedom of expression, prohibits censorship and ensures everyone's right to seek, receive and impart information taking into account the restrictions and peculiarities provided by law. Despite some legislative gaps, the Republic of Armenia provides fundamental norms to guarantee the right to freedom of expression.

92 Paragraph 7 of Article 1087.1, point 2 of Law No.239 dated 1 January 1999, the Civil Code of the RA.
93 Paragraph 7 of Article 1087.1, point 3 of Law No.239 dated 1 January 1999, the Civil Code of the RA.
94 Paragraph 8 of Article 1087.1 of Law No. 239 dated 1 January 1999, the Civil Code of the RA.
95 Paragraph 9 of Article 1087.1 of Law No. 239 dated 1 January 1999, the Civil Code of the RA.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

The Republic of Armenia is one of those states, which does not have any specific legislation on the issue of blocking and takedown of internet content. Court practice on the issue, likewise, is not established yet. Nevertheless, the issue of blocking and takedown of internet content is regulated directly and indirectly by the Constitution of the Republic of Armenia, the law on Mass Media, international agreements, treaties and conventions that are binding for the Republic of Armenia as a signatory and other domestic laws as well by other legal acts regulating relations based on them and in the framework defined by them.

According to paragraph 3 of Article 42 of the Constitution of the Republic of Armenia adopted on 6 December 2015 freedom of expression of opinion may be restricted only by law, for the purpose of state security, protecting public order, health and morals or the dignity and good reputation of others and other basic rights and freedoms thereof.[96]

Paragraph 3 of the 4th Article of the Law on Mass Media is the only national law, which directly regulates the issue of censorship of media content. In accordance with (first point of) paragraph 3 of Article 4 of the Law Censorship in the Republic of Armenia is prohibited in order to guarantee the freedom of speech in the sphere of the media.[97] According to the second point of paragraph 3 of Article 4 of the Law it is prohibited to compel the implementer of media activity or a journalist to disseminate or refrain from the dissemination of information. Taking to the account the fact that Armenian legislation does not exactly distinguish online and offline legal relations, it could be assumed that paragraph 3 of Article 4 of the Law on Mass Media refers to internet content as well and consequently prohibits internet censorship in Armenia.

While paragraph 3 of Article 4 of the Law on Mass Media regulates the prohibition of censorship of media content, it does not explicitly address the issues of blocking and takedown of media content.

Article 7 of the Law on Mass Media and Article 22 of the Law on Television and Radio set up restrictions on the freedom of speech and contain prohibited subjects for dissemination such as state or other secrets protected by the law,

96 Constitution of the Republic of Armenia 2015, Paragraph 3 of the Article 42.
97 Paragraph 3 of Article 4 of the Law dated 1 July 2004 On Mass Media.

hate speech, war propaganda, erotic/pornographic content, ethnic, religious or racial discrimination, violence and cruelty.[98]

As a member state of diverse international and regional organisations, as a signatory to numerous international and regional binding treaties and conventions that regulate blocking and takedown of internet content the Republic of Armenia must comply with its international and regional obligations and consider these international regulations before blocking and takedown of internet content.

As a member state of the United Nations the Republic of Armenia ratified The International Covenant on Civil and Political Rights (ICCPR) on 23 June 1993. According to paragraph 2 of Article 19 of ICCPR the right to freedom of expression includes freedom to seek, receive and impart all kinds of information and ideas, regardless of frontiers, either orally, written or printed, in the form of art, or through any other media of his choice.[99] Paragraph 3 of Article 19 of ICCPR does not exclude the possibility of restrictions of the freedoms mentioned in the second paragraph. Still, the restrictions should be implemented only by the law in necessity of the respect of the rights or reputations of others, the protection of national security or of the public order or of public health or morals.[100]

As a member state of The Council of Europe, Armenia signed and then ratified the European Convention on Human Rights (ECHR) on 26 April 2002. According to paragraph 2 of Article 10 of the ECHR the interests of national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, the prevention of the disclosure of information received in confidence, maintainability of the authority and impartiality of the judiciary are permissible grounds for restrictions and penalties on the freedom of expression.[101]

In accordance with part 2.2.2. of the Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States of European Council on Internet freedom any measure taken by State authorities or private-sector actors to block, filter or remove Internet content, or any request by State authorities to carry out such actions complies with the conditions of Article 10 ECHR regarding the

98 Article 7 of the Law On Mass Media.

99 Article 22 of the Law On Television and Radio.

100 International Covenant on Civil and Political Rights <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

101 The European Convention on Human Rights <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

legality, legitimacy and proportionality of restrictions.[102] Moreover, according to part 2.2.1 of the same recommendation any measure taken by State authorities or private-sector actors to block or otherwise restrict access to an entire Internet platform or information and communication, technologies, tools, or any request by State authorities to carry out such actions complies with the conditions of Article 10 of the ECHR.[103]

As a conclusion of the above-mentioned regulatory law on the issue of blocking and takedown of internet content is one of the vague areas of Armenian legislation and is scattered over several different kinds of regulation.

There is no censorship in the Republic of Armenia, Armenian government does not block or takedown internet content and generally, web content is widely reachable for Armenian internet users. Under these circumstances the severe shortage of censorship cases in Armenia is well reasoned.

However, there are still some cases related to blocking and takedown of internet content and restricted access of social networks.

The first in chronological order internet censorship case in Armenia occurred in March 2008 during post-presidential-election demonstrations, in consequence of which at least 8 people were killed, and State of Emergency was declared in Yerevan.[104] In the framework of the declared emergency some media publications, including independent internet news reporters were blocked. Pressure was applied to oppositional and independent media actors by national security services. Particularly, LiveJournal as the most prominent network used by oppositionists and activists was blocked. Although these occasions generated international criticism against Armenian government for restricting freedom of free information access, no complaint has been filed in the court concerning this case. Consequently, the case has not affected the state of the law.

In 2012 the website Armgirls.am was blocked by the Police of RA for spreading pornographic content and for offering intimate services.[105]

The third case of content removal occurred in 2015, when a regular episode of YouTube series, criticising the activities of the Police of the Republic of Armenia, was removed from YouTube.[106] Although the official reasoning of

---

102 Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom.

103 ibid.

104 Freedom House, Key Developments June 2015-May 2016, Armenia <https://freedomhouse.org/country/armenia/freedom-net/2016> accessed 26 July 2020.

105 ibid.

106 ibid.

video removal was copyright infringement (because of usage of copyrighted clip in the episode), presumably, the critics and mockery against the activities of Police of Armenia is presumed to be the real reason for the content removal. Although, a lawsuit has been field in this case.[107] The subject of the case in court was not the removal of the 11th episode of the series 'SOS', but the insult against the police publicly expressed during the release. Consequently, the following court case has no effect on the regulation of internet censorship in Armenia.

Besides, on 17 July 2016, the seizure of a police station in Yerevan by a group of opposition gunmen subsequent to their call for an armed uprising via Facebook led to inability of users to access Facebook through major ISPs, including Beeline and Ucom.[108] Access to the social network was reportedly reinstated within approximately 40 minutes.[109] This case has not influenced the state of the law too.

On 16 March 2020, at the special sitting of the National Assembly of Armenia the Prime Minister of the RA Nikol Pashinyan announced that all individuals and Armenian media outlets that disseminate false information about the corona virus, other than official information, would be subjected to liability.[110] The government explains that this aims to prevent any aggression towards patients diagnosed with corona virus or spread of panic among the population.[111] Since more than two dozen news services and some Facebook users were charged by the Armenian Police with flouting the restrictions. The Police of the RA ordered them to remove the content consisting of information, which is not fully consistent with official sources.[112] Nevertheless, Journalists, press freedom activists and opposition politicians have condemned the 'de facto censorship imposed by the authorities' claiming that the restrictions of freedom of speech are unrequired.[113] The OSCE Representative on Freedom of the Media, Harlem Désir, has also conveyed his concern regarding the above-mentioned restrictions stating that Corona virus response should not impede the work of the media in Armenia. 'I fully understand the aim of the new law to avoid panic, aggression

107 Protection of Rights without Borders NGO, The Case of "SOS" Internet Show has been Appealed to the Civil Court of Appeal <https://prwb.am/2017/05/17/sos/> accessed 26 July 2020.

108 Freedom House, Key Developments June 2015—May 2016, Armenia <https://freedomhouse.org/country/armenia/freedom-net/2016> accessed 26 July 2020.

109 ibid.

110 Aravot, Media and individuals spreading false information related to the coronavirus will be held accountable says Prime Minister <https://www.aravot.am/2020/03/16/1100330/> accessed 26 July 2020.

111 News.am, OSCE: Coronavirus response should not impede work of media in Armenia <https://news.am/eng/news/568163.html> accessed 26 July 2020.

112 Azatutyun, Yerevan Eases Coronavirus-Related Curbs On Press Freedom <https://www.azatutyun.am/a/30510768.html> accessed 26 July 2020.

113 ibid.

and to combat false information during the COVID-19 pandemic,' the Representative stated. 'At the same time, the media has a crucial role to play in providing important information to the public and to counter "fake news" on the pandemic,' Désir added.[114]

Resultantly, replying to strong criticism, on 26 March 2020, the Armenian government has significantly relieved the restrictions on the spread of information about the COVID-19 guaranteeing unrestricted operation of media outlets.[115]

Currently there are not any policy papers or proposals in the Armenian legislation for future regulation of the issue of blocking and takedown of internet content.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

3.1. Legal regulations

3.1.1. Constitutional legislation

The Constitution of the Republic of Armenia (henceforth – Constitution) provides for the ensured protection of the fundamental rights and freedoms of human beings.[116]

In the list of such freedoms and rights the freedom of expression, which is also protected on a constitutional level,[117] including almost all of its elements: freedom of opinion, freedom of information,[118] freedom of artistic expression,[119] freedom of science,[120] freedom of thought, conscience and religion[121] etc.

There is one more element, the protection of which plays a key role in the democratic society, that faces day-to-day technological advances: that is Internet freedom. The Internet has become an integral part of the everyday life all over the world. It is a space of almost unlimited opportunities, including exercising the right to expression.

---

114 OSCE, Coronavirus response should not impede the work of the media in Armenia, says OSCE Media Freedom Representative <https://www.osce.org/representative-on-freedom-of-media/449098> accessed 26 July 2020.

115 Azatutyun, Yerevan Eases Coronavirus-Related Curbs On Press Freedom <https://www.azatutyun.am/a/30510768.html> accessed 26 July 2020.

116 Article 3, The Constitution of the Republic of Armenia.

117 ibid, Article 42.

118 ibid, Article 51.

119 ibid, Article 43.

120 ibid, Article 43.

121 ibid, Article 41.

Even though Constitution covers so many aspects of the freedom of expression, its provisions cannot be considered as fully comprehensive, as there is no reference to the Internet freedom or its restrictions, including blocking or removing of Internet content.

The absence of specific constitutional norms, concerning the Internet freedom and its restrictions, namely blocking, filtering or takedown of online material, does not mean that this sphere is left unregulated. Constitutional norms serve as a legal basis for the protection of such values as state security, public order, health and morals or the honour and good reputation of others and other basic rights and freedoms not only offline, but also online.

According to Armenian legislation, the expressions, made as a result of exercising the right to freedom of expression, can be classified in two groups: (a) expressions that incorporate all elements of crime, envisaged by criminal law; and (b) expressions that are not criminally punishable but may justify a restriction and a civil suit.

The expression, that does not give rise to criminal or civil sanctions, but still raises concerns in terms of tolerance, civility and respect for others (c) is not punishable in Armenia.[122] Accordingly, the absence of legitimate grounds for blocking or removing a content that includes such expressions, does not allow to block or remove it.

Taking into consideration the fact, that there is no specific legal ground for blocking or filtering and takedown or removal of illegal internet content, and general regulations, used to provide safeguards for the rights of the addressee of such content, provide for limited mechanisms of implementation of the abovementioned processes, the content cannot be removed if it does not fall into the two categories, mentioned above (a) and (b).

3.1.2 Criminal legislation

One of the general sources of protection of a state and maintenance of legality and stability of social relations is the criminal legislation. It not only functions by exercising the penal measures, set up in the Criminal Code of the Republic of Armenia (henceforth – Criminal Code), but also serves as a general deterrent for the members of society not to be engaged in such illegal activities.[123]

---

122 UNGA, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/66/290, 10 August 2011, para. 18.

123 Article 2, Criminal Code of the Republic of Armenia.

The only ground for criminal liability is the committal a crime, envisaged by criminal law.[124]

According to Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression UNGA (10/08/2011)[125]: 'States are obliged to prohibit content falling under category (a) [mentioned above]. The category includes expression that is prohibited by international law: images of sexual exploitation of children (to protect the rights of children); advocacy of national, racial or religious hatred amounting to incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life); direct and public incitement to commit genocide (to protect the rights of affected communities); and incitement to terrorism.'

The Criminal Code stipulates the substantive grounds for the aforementioned crimes, not being limited to those. It envisages criminal liability for the threat to murder or to inflict serious damage to health or destroy property,[126] forcing a person to sexual intercourse,[127] committal of lecherous act against minor,[128] illegal collecting, keeping, use and dissemination of information pertaining to personal or family life,[129] divulging medical secrets,[130] violation of the secrecy of correspondence, telephone conversations, postal, telegraph or other communications,[131] breaching the confidentiality of ballot,[132] breach of copyright and adjacent rights,[133] breach of patent law,[134] divulging the secret of adoption,[135] illegal collection or divulging of commercial or banking secrets,[136] illegal collection or divulging of credit history,[137] inciting national, racial or religious hatred,[138] public calls for committing, financing of terrorist activity and international terrorism, public justification of terrorism,[139] crimes against computer information security,[140] illegal dissemination of pornographic materials

124 ibid, Article 3.
125 UNGA, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/66/290, 10 August 2011, paras. 20-36.
126 Article 137 of the Criminal Code of the Republic of Armenia.
127 ibid, Article 140.
128 ibid, Article 142.
129 ibid, Article 144.
130 ibid, Article 145.
131 ibid, Article 146.
132 ibid, Article 154.
133 ibid, Article 158.
134 ibid, Article 159.
135 ibid, Article 169.
136 Article 199 of Criminal Code of the Republic of Armenia.
137 ibid, Article 199.1.
138 ibid, Article 226.
139 ibid, Article 226.1.
140 ibid, Chapter 24.

or items,[141] public calls for changing the constitutional order of the Republic of Armenia by force, seizure of the power and breaching territorial integrity,[142] divulging a state secret,[143] divulging the data of inquiry or investigation,[144] contemptuous treatment of court,[145] slandering the judge, the prosecutor, the investigator or the person in charge of inquiry, marshal of the court,[146] threat or violence in relation to preliminary investigation or administration of justice,[147] insulting a serviceman,[148] public calls for aggressive war,[149] denying, mitigating, approving or justifying genocide and other crimes against humanity.[150]

There is no specific decision-making process by investigative bodies about removal or blocking of an illegal content, that incorporates elements of crime in it. Thus, again general regulations are in place to provide for legal grounds for blocking or removing the allegedly illegal content from the Internet both during the pre-trial investigation and the trial itself, until the court determines whether the act contains all the elements of crime and is the accused person criminally liable for it.

Internet service providers and telecommunication operators are not obliged to check whether the published material contains illegal content or not.[151] Thus, they cannot be liable for transmitting illegal content. But this regulation does not apply for every single situation. Particularly the main condition, under which the Internet provider can be liable for publishing the illegal content, is when he or she has prior knowledge of it.

However, Internet service providers and telecommunication operators are bound to open access to law enforcement bodies for conducting surveillance. The decision for conducting surveillance over internet content must be taken by court on the basis of the motion by the investigator of the Investigative Committee of Armenia or the NSS to court.[152] As a result of the surveillance, these bodies may decide to start criminal prosecution or cancel the proceedings for the lack of crime. The decision of the investigator can be appealed to the

141 ibid, Article 263.
142 ibid, Article 301.
143 ibid, Article 306.
144 ibid, Article 342.
145 ibid, Article 343.
146 ibid, Article 344.
147 ibid, Article 347.
148 ibid, Article 360.
149 ibid, Article 385.
150 Article 397.1 of Criminal Code of the Republic of Armenia.
151 Article 2 of the Law of the Republic of Armenia on Electronic Communications.
152 Article 50 of the Law of the Republic of Armenia on Electronic Communications, Article 278, Criminal Procedure Code of the Republic of Armenia.

supervising prosecutor and further to the court of the prosecutor refuses the appeal.[153]

During the pre-trial investigation and if the webpage is hosted in Armenia, the investigator may seize the telecommunication devices located at intermediary's premises. The seizure is done for the purpose of conducting forensic examination of the hardware or the software as far as it concerns the alleged illegal content. As a result of the seizure, the content is automatically blocked and remains as such until the final court decision on the merits is made. So, the decision on seizure accidentally plays the role of temporary injunction.[154]

Armenian criminal legislation provides for limited legal basis for exercising restrictions on the freedom of expression, which may be applied on the Internet in compliance with the ECHR case law measures. And the protection of state security, protecting public order, health and morals or the honour and good reputation of others and other basic rights and freedoms serves as the legitimate aim for such actions.

Neither the Criminal Code, nor the Criminal Procedure Code provide the freedom of expression safeguards such as the principles of proportionality and necessity of measures,[155] although according to ECtHR assessments these issues must be examined by the court.[156]

Even though is not in Armenian legal culture to apply freedom of expression safeguards in criminal proceedings[157], but accepting and complying its legislation and practice to the ECHR case law is a constitutional obligation.[158]

But despite that binding provision, ECHR case law is not cited by parties in criminal proceedings specifically in cases, involving internet content.

Thus, at this point there is no comprehensive legal approach to restricting the freedom of expression, including Internet freedom. Public authorities in Armenia must rely on the existing general legislative regulations for ensuring the protection of human and citizens' rights and freedoms, the rights of legal entities, property, the environment, public order and security, constitutional order from crimes, committed online.

---

153 Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015, page 32.

154 ibid, page 32-33.

155 Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015, page 33.

156 Jersild v. Denmark; Hertel v. Switzerland, 25 August 1998 and Steel and Morris v. the United Kingdom.

157 Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015, page 29.

158 Article 81 of the Constitution of the Republic of Armenia.

3.1.3 Civil legislation

Expressions that are not criminally punishable, but may justify a restriction and a civil suit, are also considered as circumventions of the restrictions on the freedom of expression.

The Civil Code of the Republic of Armenia (henceforth – Civil Code) provides for sufficient legal grounds for considering an internet content as violation of others' rights. But the situation, concerning the legal regulations of blocking or filtering and takedown or removal of illegal internet content, is similar to the one in criminal sphere. There are no specific regulations about limitations on Internet freedom: the only means of prevention of circumvention of the restrictions on the freedom of expression are the general regulations of civil legislation.

The civil laws provide detailed substantive law grounds for declaring as illegal such content as defamation, insult[159], copyright violation[160] etc. There is no effective framework in the Civil Code for ordering content removal or content blocking as measures of civil remedy[161] Civil Code does not provide direct regulations due to which one can protect his or her rights by the direct claim of removing or blocking an illegal content. Anyway, the victim of an insult or a slander can make a claim, requiring public apology in the case of an insult or requiring public refutation of factual data, considered as slander and (or) publication of its response with regard thereto. The form of apology or refutation and (or) publication shall be defined and approved by the Court. Particularly, the form of public refutation of factual data, considered as slander, and (or) publication of its response with regard thereto, shall be approved by the court, guided by the Law of the Republic of Armenia 'On Mass Media'.[162] As blocking or removal of an insult or defamation can lead to restoration of the situation, that existed before insulting or defaming the victim or can prevent violations or the threat of the violations against the rights of the victim, he or she can protect his or her rights, relying on the ways of protection, established in the section 2 and section 3 of Article 14 of Civil Code. Thus, Civil Code does not include a provision, that will give the victim a right to address a direct claim of removing or blocking an allegedly illegal content: he or she can do it, based on the general regulations, which are mentioned above.

---

159 Article 1087.1 of the Civil Code of the Republic of Armenia.

160 Article 66 of the Law of the Republic of Armenia on Copyright and Related Rights.

161 Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015, page 33.

162 Article 1087.1, section subsection 1 of 7, subsection 1 of section 8 of Civil Code of the Republic of Armenia, Article 8, of the Law of the Republic of Armenia On mass media.

The subjects of civil relations acquire and exercise their civil rights upon their will and to their benefit.[163]Although Civil Code provides for the protection of the subject's honour, dignity and business reputation,[164] but the one, who can take action for the protection of those values, is the citizen or the legal person whose rights are violated as a result of a misdemeanour or tort by another subject, who circumvented the restrictions on the freedom of expression, using the means of protection, established in the Civil Code.[165]

If a civil offence, done by violating one's right to reputation, right to intellectual property, right to protection of personal data or other related rights, took place, these ways of protection, established in the Article 14 of Civil Code, can be applied: restoration of the situation having existed before the violation of the right (2), prevention of actions violating the right or creating a threat for the violation thereof (3), self-protection of the right (8), compensation for damages (10). As the list of the means of protection in Civil Code is not exhaustive, civil rights of the victims can be recovered and protected by other ways provided for by law (13).

The legislator provides for the opportunity of protection of the rights (51), which may include demanding compensation of both pecuniary and non-pecuniary damages, resulting from an insult or defamation. The victim of such offence can protect his or her rights by judicial or non-judicial means.

Taking-down and blocking of the illegal content as a civil remedy can be ordered by court on the basis of the Article 14 of the Civil Code defining the exhaustive list of civil remedies and among them two remedies under subsections 2 and 3 'to reinstate the situation that existed before the violation' and 'to prevent the actions that violated the rights or created a threat to its violation' accordingly.

If the victim required non-judicial protection[166] and the refutation was done, he or she cannot apply to the court, demanding compensation of pecuniary and (or) non-pecuniary damages, resulted from the civil offence, as there's a reasonable allegation that his or her rights are already protected by means of non-judicial method.

Civil Code also provides for exceptions from liability for insult or defamation. Namely, if the information about the initial source of published information is disclosed, then the publisher will not be punished[53], but if the author of

163 Article 3 and Article 11 of Civil Code of the Republic of Armenia.
164 Ibid, Article 19, Article 162.
165 Article 14 of Civil Code of the Republic of Armenia.
166 Article 1087.1, section 6 of Civil Code of the Republic of Armenia.

insulting or defamatory content is not disclosed, it serves a guarantee for the protection of the rights of an addressee of an insult or defamation.[167]

There's no definite provision, that will give an opportunity to demand blocking/filtering/ or takedown/removal/ of illegal internet content, but it can be done by requiring some ways of protection, established in the Article 14 of Civil Code. Although there has been a legislative initiative in 2014, concerning the This gap in the law was the reason, including the Chamber judgment of the European Court of Human Rights in Delfi case in October 2013, that two members of the Parliament introduced a bill of amendments to the Article 1087.1 of the Civil Code (a supplementing Article 1087.2) by which they proposed to add specific reference to content removal in the text of the article as a remedial measure. The bill introduced also liability of online media entities for third-party defamatory comments published on the portal of the entity by anonymous or fake account holders which is very wide practice in Armenia. The bill was admitted by civil society with strong criticism. The media community contended that the bill would jeopardise the free speech on internet. On 14/03/2014, nine journalistic associations disseminated a joint statement urging the parliamentarians to withdraw the initiative.[168] On 30 March 2014, Reporters Without Borders (RSF) urged the parliamentarians to withdraw the draft law and support the solution of the problem through self-regulatory mechanisms.[169] Under pressure of the civil society, the parliamentarians withdrew the bill for an indefinite period of time.[170]

In cases of defamation, slander and insult, violation of privacy and copyright, the court may order blocking of content during trial as a temporary injunction or may rule on the merits by blocking the content as a judicial remedy. Blocking the content as a civil remedy can be ordered by court on the basis of the Article 14 of the Civil Code defining the exhaustive list of civil remedies and among them two remedies under subsections 2 and 3 'to reinstate the situation that existed before the violation' and 'to prevent the actions that violated the rights or created a threat to its violation' accordingly.

Copyright Law also provides special regulations for the protection of copyright in Internet for those cases when one uses information, making quotations from

---

167 Ibid, Article 1087.1, section 9.

168 Yerevan Press Club, Journalistic Associations Believe Draft Law on "Fake Accounts" Will Cause New Problems <http://ypc.am/oldypc/bulletin/t/45853/ln/en> accessed on 28 July 2020.

169 Reporters Without Borders, Armenia bill poses danger to online <https://en.rsf.org/armenia-bill-poses-danger-to-online-30-03 2014,46060.html> accessed 28 July 2020.

170 Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015, page 31.

newspaper articles or periodicals, published on the Internet. According to section 1 and section 2 of Article 22.1 of Copyright Law one can freely make quotations from the above-mentioned works, provided that the extent of quotations is justified by the purpose and does not have negative effect on the number of the viewers and the extent of use of the original work, and also that the quotation does not express the essential part of the initial work. According to the same article, mention shall be made of the source, and of the name of the author if it appears thereon. It is also stated that the work can be fully implemented from newspaper articles or periodicals, provided that it has been agreed upon with the author of the original work. In these cases, the victim can protect his or her rights, relying on the Article 14 of the Civil Code. The victim can also demand compensation for the damages, according to subsection (d) of section 1 of Article 66 of Copyright Law.

A party winning the case may ask the court to issue a writ of execution on the basis of which the body responsible for enforcement of court decisions (Department of Enforcement of Judicial Acts under the Ministry of Justice (DEJA)) has to institute enforcement proceedings and request the telecommunication operator, the ISP (Internet Service Provider) or the host provider to block [or remove] the certain content.[171]

Therefore, the ISPs or the operators have no choice but to comply with the request. Despite the above remedial measures specified in the Civil Code and the Law on Copyrights and Related Rights, no specific safeguards for freedom of expression in relation to blocking of content are stipulated in them,[172] nor do they provide for comprehensive legislative basis for removal of internet content that contains defamatory or insulting expressions or violations of copyright or related rights.

3.1.4. Other legislation

According to constitutional[173] and other legislative norms[174] freedom of expression may be limited for ensuring the state emergency.

Taking into consideration the situation, concerning the quick spread of the corona virus (Covid-19) and its possible consequences, the Republic of Armenia declared a state of emergency on 16/03/2020.[175] As a result of that action, some

171 Article 71, the Law on Compulsory Enforcement of Court Orders.
172 Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015, page 27.
173 Article 76 of the Constitution of the Republic of Armenia.
174 Law on Legal Regime of the State of Emergency.
175 Decision of the Government of the Republic of Armenia on Declaring a State of Emergency in the Republic of Armenia, N 298-Ա.

limitations have been put on the population, including restrictions on the freedom of expression. Although the limitations on the right to expression did not last as long as the other ones, they still arose controversies over the definition of spreading the information that causes panic or creates real danger of panic situations among the population. Journalists and editors have criticised this decision, stating that there is no precise definition of which messages may or may not cause panic.[176] The limitation on the freedom of expression were in force until 13/04/2020.

Law on Legal Regime of the State of Emergency complies with the requirements of ECHR about the measures of restrictions on the freedom of expression, as the law sets strong guarantees against arbitrariness such as the principle of proportionality and relevancy of measures, the requirement of rational link between the measure and the legitimate aim sought.[177]

The decision on content blocking on the abovementioned ground is an administrative act, and the regulations are in compliance with ECHR case law, concerning the safeguarding mechanisms to prevent violations of others' rights.

The Law on Fundamentals of Administration and Administrative Procedure provides for safeguards in the cases blocking the allegedly illegal content in the name of the fundamental principles of administrative action. Among those the principle of legality, the principle of limitation of discretionary powers, the principle of arbitrariness, the principle of efficiency, the principle of proportionality[178] are the ones, that guarantee the effective protection of the freedom of expression. These principles serve as a legal basis for the administrative and judicial bodies, when they should make a decision about legality and proportionality of the limitation on the right to expression, including blocking or removal an allegedly illegal content, as the threshold for such these cases is not explicitly mentioned in the Law on Fundamentals of Administration and Administrative Procedure

If the subjects of the administrative act are displeased with the administrative act, it can be challenged to the higher administrative body or straight to the Administrative Court. If the claimant is not satisfied with the decision of the

176 OSCE, Coronavirus response should not impede the work of the media in Armenia, says OSCE Media Freedom Representative <https://www.osce.org/representative-on-freedom-of-media/449098?fbclid=IwAR0s8HwZmb0Nz9788kW6Lq6vWTn3ZLxcnkFmcCCO3p2HpREk2HOHrCkHVYM> accessed 28 July 2020.

177 Article 10 of Law on Legal Regime of the State of Emergency.

178 Articles 4, 6-8, 11 of the Law on Fundamentals of Administration and Administrative Procedure.

court, it can be appealed to the Administrative Appeal Court, then to the Court of Cassation of Armenia.

The right to protection of personal data, protected by Constitution,[179] can also be violated as a result of exercising the freedom of expression.

Law of the Republic of Armenia on Protection of Personal Data (henceforth - Personal Data Protection Law) contains more detailed regulations about restrictions on the right and the safeguards, which are in compliance with the ECHR case law, as they provide for mechanisms for balancing both the Right to Expression and the Right to Protection of Personal Data.[180]

The data subject has the right to information, concerning the processing of his personal data and its compliance to the aforementioned measures. If the there is any incompliance to the criteria, the data subject has the right to require blocking or removal (destruction) of such information.[181]

Armenian legislation gives the data subjects an opportunity to require blocking or removing of their personal data, which contain information, that is incomplete or inaccurate or outdated or unlawfully obtained or unnecessary for achieving the purposes of the processing.

If the breach of personal data contains elements of crime in it, then the process of examination will be in accordance with the Criminal Procedure Code as follows in 1.2. But if it is only an administrative offence and does not incorporate all elements of crime, envisaged by Criminal Code, and if the data subject suffered pecuniary and (or) non-pecuniary damages, resulting from that offence, he or she can claim for compensation for those damages in accordance with the Civil Code and Civil Procedure Code as follows in 1.3.

3.2. Case Law

In Armenia there is nearly no sufficient legal basis for blocking or filtering and takedown or removal of internet content, taking into account the aforementioned legal regulations.

The absence of legislation regarding to blocking or removal of internet content has led to almost the same situation in the case law.

Although the supreme court instance – the Cassation Court of the Republic of Armenia[182] and Constitutional Court, which play a key role in interpreting

179 Article 34 of the Constitution of the Republic of Armenia.
180 Article 5-8,16 of the Law of the Republic of Armenia on Protection of Personal Data
181 Ibid, Article 15
182 Article 171 of the Constitution of the Republic of Armenia.

Armenian legislation, issued precedents and decisions, concerning the cases where there was a defamatory or insulting internet content, those decisions actually do not directly obligate authorities to apply such civil remedies, as blocking or removing of illegal internet content. They only indirectly obligate authorities to operate in accordance with case law of ECHR concerning Article 10 of the Convention, including such underlying principles as the necessity to democratic society, the proportionality and relevancy of measures, the balancing test between the public interest and the interest of the individual, legitimacy of the purpose of interference, the grounds under which the public interest prevails such as the wide scope of permissible criticism of politicians and public figures, the special role of media and its wide protection under Article 10, protection of the speech contributing to general public debates, unacceptability of rendering protection to certain speech such as hate speech, intolerance, racist remarks, etc. conflicting with democratic values.[183]

Thus, taking into consideration the assessments of the ECtHR, particularly concerning limitations on the freedom of expression online, is a constitutional obligation, which is not always performed by public authorities.

Only in the case of *Artur Grigoryan v. 'Hraparak' daily newspaper LLC*,[184] during which Arthur Grigoryan was demanding compensation of damages for insults and defamation, that were under the online publication of 'Hraparak' daily newspaper, there is a reference to the mechanisms of removal of illegal content (but there is no application of the mechanisms). In the final decision the Court of first instance of Kentron and Nork-Marash regions asserted that the newspaper had no guilt in making the defamatory and insulting statements: its main function was publishing the news, which was conducted for public interests. What concerns the removal of comments, that involved illegal content and violated Arthur Grigoryan's right to honour, dignity and business reputation, it is not obligatory for the newspaper to remove those comments if there's no notice about it from an average user, namely Arthur Grigoryan in this case. In this decision, the court referred to the case of *Delfi AS v. Estonia*,[185] in which the European Court of Human Rights provides for the measures for blocking or removing of the Internet content. Despite the absence of incorporated legal mechanisms for conducting notice-and-take-down system,

[183] Constitutional Court decision no. SDV-997 of 11 November 2011, at section 10. /cited from Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015, page 30/.

[184] Case of *Artur Grigoryan v. 'Hraparak' daily newspaper LLC*, First Instance Court of General Jurisdiction of Kentron and Nork-Marash districts, case no. EKD/2491/02/11 ("ԵԿԴ/2491/02/11"), 7 March 2012.

[185] *Delfi AS v. Estonia* (Application no. 64569/09), judgment of 16 June 2015, para. 159.

the court, referring to it and taking into account the constitutional obligation of complying to ECHR case law, decided that 'Hraparak' daily newspaper was not guilty in publishing the abusive comments, as there was no notice from Arthur Grigoryan to remove the information and publishing of the material was aimed at satisfying public interests.

There is no case law about blocking or removing an illegal content and protecting the victim from the breaches against copyright.

Despite the absence of regulations, recently some actions have been taken by the public authorities for removing allegedly illegal internet content. One of such cases is the detention of the supposed owner of the web-page under the name 'Duxov Hayastan – open society' ('Դուխով Հայաստան – բաց հասարակություն') on Facebook, the publications of which included hate speech, punishable under Criminal Code[186]. The protection of national security was brought forward as a legitimate ground to justify the actions of the authorities, affirming their necessity and proportionality, constituted by ECHR case law.[187]

Another case, similar to the previous one, is the case of a fake page under the name of 'Diana Harutyunyan' on Facebook, spreading false information in order to defame present-day authorities, as the suspected stated.[188] It particularly reported, that Armenian Prime Minister Nikol Pashinyan had congratulated the US President on the action taken against Iran's top military, which was considered as an act, inciting national, racial and religious hostility, significantly damaging the national security interests of the Republic of Armenia.[189] Operative-intelligence activities were carried out by the RA National Security Service, the identity of the host of 'Diana Harutyunyan' Facebook page was revealed and the person who allegedly operated the page, has been detained: he is suspected of committing crimes which are established in the Criminal Code.[190]

Despite the legitimate aim, in both cases public authorities took actions against publications on the Internet, that contained illegal content, by detaining the alleged penetrators. Taking into consideration the regulations of the Criminal Procedure Code, the supposed illegal content may be blocked or removed from

186 Article 226 of the Criminal Code of the Republic of Armenia.

187 The person leading the Facebook page of the Open Society of Spirits Hayastan on Facebook - Director of the National Security Service <https://rus.azatutyun.am/a/29863984.html> accessed 28 July 2020.

188 Armen Press, Man who deliberately spread fake news about Soleimani in Armenia indicted and jailed <https://armenpress.am/eng/news/1000724.html> accessed 28 July 2020.

189 Iravaban, Host of Diana Harutyunyan Fake Facebook Page arrested: NSS <https://iravaban.net/en/252287.html> accessed 28 July 2020.

190 Article 226 and Article 254 of the Criminal Code of the Republic of Armenia.

online sphere for the sake of state emergency, as a legitimate ground. As it was already mentioned, the regulations for blocking or removing internet content are very vague and almost non-existent, so in this sense the operations of the authorities may be considered unlawful actions.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

The regulation of online content is challenging, and more and more states are adopting laws aimed at regulating the web, thereby threatening media pluralism. To avoid state interference with the right to freedom of expression online, some have been encouraging the online industry to address illegal content or copyright issues on the cyberspace through 'self-regulation'.[191] Armenia is not an exception; the national legislation provides for the opportunity of online content self-regulation in several ways.

The RA law 'On Mass Media' (hereinafter, the 'Law') provides a specific mass media oriented regulation. Expressly prohibiting censorship (Article 4(3) of the Law), the Law prescribes for the mechanisms of illegal content takedown.

As mentioned under section (1), according to Article 8 of the Law, a person has a right to demand that the mass media activity implementer refute factual inaccuracies in the information disseminated thereby if the latter does not prove the truth of those facts. The demand for refutation has to be presented within one-month period following the day of publication of the information subject to refutation. Within one week after a refutation demand receipt the mass media activity implementer shall notify the refuting party of the time of the refutation dissemination or send a written refusal to publish the refutation. The refutation shall be disseminated by the same media product, or if impossible, another acceptable means for the refuting party shall be identified. It shall be published within a period of one week following the day of its receipt. If within this period the media product is not issued or the subsequent issue has already been endorsed for publication, the refutation is to be published and disseminated in the nearest issue of the media product. Refutation shall be placed under the title 'Refutation'. Its placement, layout, font size and type, the time of broadcasting should not be different from the information being refuted.

191 OSCE, The Online Media Self-Regulation Guidebook <https://www.osce.org/fom/99560?download=true> accessed 29 February 2020.

The same Article provides for a specific regulation for elections: during elections of state and local self-government bodies the refutation of information about candidates shall be effected within 24 hours. If less than 24 hours remain until the commencement of voting, the refutation shall result immediately upon its receipt. If the dissemination of the refutation is impossible, it has to be disseminated within the timeframe stipulated in the Article.

Along with refutation, a person has the right to demand publishing of a response. The implementer of media activities may choose to accompany or not the publishing of the response along with refutation. By publication of the response, the right to refutation is considered to be fulfilled. The publication of the response shall be carried out in accordance with the rules stipulated for refutation.

The same Article establishes additional requirements for the response as well. The response shall refer solely to the actual inaccuracies in the information subject to response. It shall not contain criticism of the person who had prepared or disseminated the information, any other person or their activities if it is not directly pertinent to that information. The volume of the response shall not exceed the volume of the material being responded to. If the refuted information is a separate, clearly divisible section from the whole volume of the material, then the response volume shall not exceed the volume of that section. The response shall be published free of charge. The law provides for the grounds for refutation and/ or response publication denial, which are discussed under section 1 hereof.

The refuting person has also a right of judicial protection. Under Article 8(9) if a mass media implementer refuses to publish the refutation or the response, or infringes the terms and procedures of their dissemination as provided by the Law, the person whose rights are violated has a right to file a lawsuit demanding to disseminate the refutation or response.

Under sub clause 1 of Article 1087.1 of the Civil Code of the Republic of Armenia (hereafter, the 'CC'), the person whose honour, dignity or business reputation have been disgraced through insult or slander, may apply to court against the person having insulted or slandered.

According to sub clause 2 of the same Article, in the scope of CC, insult shall be deemed as a public statement made with the purpose of disgracing the honour, dignity or business reputation through speech, image, voice, sign or other means. Public statement may not be deemed as an insult in the given situation and by virtue of its content where it is based on accurate facts (except for congenital disorders) or is conditioned by overriding public interest. Under clause 3 of the

said Article, slander shall be deemed as public communication of factual data (statement of fact) relating to a person, which does not correspond to the reality and disgrace the honour, dignity or business reputation thereof.

As it can be construed, in the scope of CC, both insult and slander are public in their nature, hence, the aforementioned regulation is applicable to the issues arising out of illegal content (insult or slander) published on the Internet. The regulation prescribed for by the CC stipulates that a lawsuit under said Article may be filed with the court within one month after the person has become aware of the insult or slander, but not later than within six months from the moment of the insult or slander.

The RA Court of Cassation has rendered a few decisions of a precedential character regarding the manner of rights protection on such matters, expressly stating that the injured person shall choose the manner of their rights protection, whether by demanding a refutation by the mass media product (extrajudicial manner) or via filing a lawsuit with a court on its own discretion. In any case, the lawsuit shall be submitted not later than before expiration of a 6-month term after the moment of the insult or slander and within one month after being informed thereof.

Under the acting legislation, upon expiration of a 6-month term the person is still entitled to invoke its rights of protection, however a notice to the mass media implementer will no longer be binding for them. As for a lawsuit, should the respondent claim on expiration of a 6-month term and such fact confirmed, the lawsuit shall be rejected in full as stipulated under Article 168 (6) of Civil Procedure Code of the Republic of Armenia.

So, the acting legislation provides for special measures of self-regulation of published content in both extrajudicial and judicial manner, which can be implemented in the form of publishing a refutation and/ or a response.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

The Internet made vast changes in our lives in the era of informational technologies and their constant development. People have become more addicted to post their life, so it has become harder to keep track even of their own activities, done on the Internet before.

The issue of the possibility of their permanent erasure arises after the publications of such activities. The opportunity of deleting the online materials,

containing personal information, can be provided by 'the right to be forgotten' or 'the right to erasure'. The day-to-day rise of the influence of the Internet on people's lives is directly proportional to the rise of the importance of the mentioned rights, as the protection of private materials can be ensured by them.

The right to be forgotten derives from the case Google Spain SL, *Google Inc v. Agencia Española de Protección de Datos*, Mario Costeja González (2014). It has firstly been codified in the General Data Protection Regulation (GDPR) in addition to the right to erasure.[192]

While social media is all about making a mark, about saying 'This is me', the right to be forgotten is about handing over a different kind of power. It is the assertion of ownership of one's own identity by refusing to give ownership to the platforms that published the posts.[193]

Right to be Forgotten or Right to Erasure is one of the key privacy rights, as the data controller must follow the requirements of the data subject to delete his or her personal data, if there are sufficient legal grounds for that, namely, as it is established in the GDPR, Article 17, the personal data must be erased immediately where the data are no longer needed for their original processing purpose, or the data subject has withdrawn his consent and there is no other legal ground for processing, the data subject has objected and there are no overriding legitimate grounds for the processing, or erasure is required to fulfil a statutory obligation under the EU law or the right of the Member States. In addition, data must naturally be erased if the processing itself was against the law in the first place.[194]

Armenia does not apply specific legislation on the 'right to be forgotten' or the 'right to delete'. Only the Law of the Republic of Armenia on Protection of Personal Data (henceforth - Personal Data Protection Law) contains provisions about restrictions on processing personal data, which can be interpreted as the right of the data subject to be forgotten.

According to Article 1, section 1 of Personal Data Protection Law:

'This Law shall regulate the procedure and conditions for processing personal data, exercising state control over them by state administration or local self-

192 Article 17 of the GDPR.

193 Suzanne Moore, The right to be forgotten is the right to have an imperfect past <https://www.theguardian.com/commentisfree/2017/aug/07/right-to-be-forgotten-data-protection-bill-ownership-identity-facebook-google>.

194 Intersoft Consulting, Right to be Forgotten <https://gdpr-info.eu/issues/right-to-be-forgotten/>.

government bodies, state or community institutions or organisations, legal or natural persons.'

According to Article 15, section of Personal Data Protection Law:

'1. The data subject shall have the right to information on his or her personal data, processing of data, grounds and purposes for processing, processor of data, the registered office thereof, as well as the scope of persons to whom personal data may be transferred.

2. The data subject shall have the right to get familiarised with his or her personal data, require from the processor to rectify, block or destruct his or her personal data, where the personal data are not complete or accurate or are outdated or have been obtained unlawfully or are not necessary for achieving the purposes of the processing.

3. In case of doubts with regard to the rectification, blocking or destruction of personal data by the processor, the data subject shall have the right to apply to the authorised body for the protection of personal data to make clear the fact of his or her personal data being rectified, blocked or destructed and by the request to be provided with information.'

The definitions of blocking and destruction of personal data are given in the Article 3, section 1, subsections 10-11, as follows:

'1. The following main concepts shall be used in this Law:

(…);

(10) blocking of personal data - temporary suspension of the possibility to collect or fix or systematise or transfer or use personal data;

(11) destruction of personal data - an operation, which renders the restoration of the content of personal data contained in an information system impossible;

(…).'

According to Article 17, section of Personal Data Protection Law:

'1. Where the data subject considers that the processing of his or her personal data is carried out in violation of the requirements of this Law or otherwise violates his or her rights and freedoms, he or she shall have the right to appeal actions or inaction of the processor before an authorised state body for the protection of personal data or through judicial procedure.

2. The data subject shall have the right to compensation of damage as prescribed by law.'

The regulations of European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are binding for Armenia as a member of The Council of Europe. [195] Article 8 of the convention provides the data subject with safeguards for the protection of his or her personal data, including the right to require erasure of personal data.

Armenian legislation gives data subjects an opportunity to require blocking or removing of their personal data, where the data are not complete or accurate or are outdated or have been obtained unlawfully or are not necessary for achieving the purposes of the processing. This provision may be considered as the interpretation of the right to be forgotten or the right to erasure, as the grounds for requiring the erasure of personal materials are similar to the criteria, set in the GDPR. If the processing of personal data is carried out unlawfully, then the data subject shall have the right to appeal actions processor of his personal data before an authorised state body of personal data or straight through judicial procedure for the protection of his or her privacy rights.

As the existing domestic regulations do not provide explicit and clear legal ground for the protection of the right to be forgotten or right to erasure, there is also no court practice, related to it.

The right to be forgotten is a new phenomenon all over the world: Armenia is not an exception. It is scarcely observed and interpreted both by competent authors and law theorists. Armenian Lawyers' Association concluded in its report[196] that Armenian legislation on Personal Data Protection is incomplete, as it does not contain provisions that would cover the right to delete personal data, which, in spite of being obtained lawfully, can create a direct threaten to an individual's rights and is not proportional to the legitimate aims (page 11, para. 2), or the right to delete information about formerly having committed misdemeanour, civil offence or not serious crime from web-pages after the court issues the final decision about the case (page 11, para. 3), or the right to require erasure of abusive or personal information (including personal page) about an individual, who is dead or is declared as missing or dead, which is to be exercised by his or her relatives (page 11, para. 4) etc.

In summary, although Armenia does not apply specific legislation on the 'right to be forgotten' or the 'right to delete', it is provided for explicit and clear protection of the right to be forgotten or the right to delete data subjects.

---

[195] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data <https://rm.coe.int/1680078b37>.

[196] Armenian Lawyers' Association Report <https://armla.am/wpcontent/uploads/2019/01/Առռացված-լինելու-իրավունք-Նարեկ.pdf>.

6. How does your country regulate the liability of internet intermediaries?

According to the Armenian legislation the internet intermediaries (internet service providers) are not obliged to control and edit the information flow, including the choice of media content, its takedown, publishing, amendments, etc.[197] On the contrary, any censorship is prohibited by virtue of law. Thus, under Armenian legislation, the internet intermediaries cannot be liable for the illegal content published on the Internet. The only exception is established by the Law on Electronic Communication, when the intermediary itself allows spread of information dangerous for the society – containing elements of crime. According to Article 51, an intermediary who deliberately allows their network or services to be used by a person to deceive other persons or to use violence, malice, threats or blackmail against other persons, shall be subject to a penalty, which shall not exceed AMD 5 million, and which shall be imposed by the Public Services Regulatory Commission of the Republic of Armenia. Considering that the Article directly refers to the activities of criminal nature, we can say that its action requires a final and binding court decision confirming the fact of the crime(s), intermediary's awareness and allowance of that exact crime(s). Since the Armenian legislation does not impose liability on legal entities for crimes, this regulation can be considered as an alternative to impose penalties on intermediaries for involvement in such crime-related activities.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

According to Recommendation CM/Rec (2016) 5(1) of the Committee of Ministers to member states on Internet freedom: 'The European Convention on Human Rights applies both offline and online. The Council of Europe member States have negative and positive obligations to respect, protect and promote human rights and fundamental freedoms on the Internet'.[198] Basically, the State has an obligation of providing protection for all of the spectrum of Human Rights both online and offline. So far, these are the legislative acts, that have

---

197 The Best in the Net. online journalist's guidebook <https://www.osce.org/hy/yerevan/109869?download=true>, accessed 29 February 2020.

198 Recommendation CM/Rec (2016) 5(1) of the Committee of Ministers to Member States on Internet Freedom <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa>.

been adopted by Armenia regarding online content blocking and take-down and liability of Internet intermediaries;

'Law of 13/12/2003 on Mass Media',

'Law of 23/09/2003 on Freedom of Information',

'Law of 18/05/2015 on Protection of personal data',

'Criminal procedure code of 01/071998',

'Criminal code of 18/04/2003',

'Law of 03/121996 on State and Official secrets',

'Law of 22/10/2007 on Operational-Intelligence activities',

'Decision of the Government of 31/07/2008 of the Republic of Armenia on conducting operative-intelligence activities; Confirmation of the list of specially (designed, programmed, customized) technical tools',

'Law of 13/08/2005 on Electronic communication',

'Law of 15/06/2006 on Copyright and related rights',

'Law of 09/102000 on Television and radio'.

It is clear that Armenia is not among the countries which have specific legislation regarding Internet censorship, and different laws cover different aspects of the matter. Sometimes provisions in different laws contradict themselves and Armenian legislation will have a period of harmonizing its provisions regarding online content blocking and take-down and liability of Internet intermediaries.

The Armenian legislation does not have provisions regarding liability of Internet intermediaries and there are no grounds for claiming that there will be changes in this respect.

Armenian legislation has not properly responded to the emerging right to be forgotten, which will be quiet problematic because of the low personal data protection level that the Armenian government provides for its citizens (e.g. elections.am web-site which provides a large range of personal data about Armenian citizens who have right to vote in free access online). Armenia fails in this context to find a balance between transparency and personal data protection. Thus, for providing the possibility to exercise the right to be forgotten, Armenia needs to rethink its policy and approach to personal data protection.

Therefore, the main domains of developments will be harmonizing the legislation to avoid contradictions and providing guarantees for personal data protection.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

In the 21st century, the Internet enables every person to search, find, disseminate any information, express their thoughts, ideas. In any democratic country, this is an important guarantee of the right to freedom of expression. However, this right is abused very often, especially on online domains, and that turns freedom of expression into hate speech for one to another group.

There is no unified definition of hate speech.

The Committee of Ministers of the Council of Europe provides the definition of hate speech 'The term 'hate speech' shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin. The governments of the member states, public authorities and public institutions at the national, regional and local levels, as well as officials, have special responsibility to refrain from statements, in particular to the media, which may reasonably be understood as hate speech, or as speech likely to produce the effect of legitimizing, spreading or promoting racial hatred, xenophobia, anti-Semitism or other forms of discrimination or hatred based on intolerance. Such statements should be prohibited and publicly disavowed whenever they occur'.[199]

The Republic of Armenia guarantees the Right to Freedom of Expression at the constitutional level. At the same time, it stipulates that human dignity is an inalienable basis of their rights and freedoms. However, there are cases, when individuals on the Internet, assuming they exercise their right to freedom of expression, disseminate expressions and ideas that infringe on human dignity and honour and preach hate speech to one or another group or individuals.

The RA legislation regulates the cases, when a person denies, mitigates, approves or justifies the genocide and other crimes against peace and human security. According to the Article 397[1] of the Criminal Code of the Republic of Armenia the dissemination of materials to the public through the computer system or making them available in any other way, denying, mitigating, approving or justifying genocide and crimes against peace and security of humanity under

[199] Recommendation No R 97(20) 30 October (1997), page 108 <https://rm.coe.int/opening-session-2-parmar-the-legal-framework-for-addressing-hate-speec/16808ee4bf> accessed 27 May 2020.

other Articles of this chapter, if committed on the basis of racial affiliation, colour, national or ethnic origin or on the basis of religious affiliation to incite hatred, discrimination or violence against a person or group of persons is punishable by a fine in the amount of 300-fold of the defined minimum salary, or imprisonment for a maximum of four years. This means that the RA Criminal Code bans the dissemination, denial, mitigation, approval or justification of the genocide or crimes against peace and security of humanity through computer system, which includes the dissemination on the internet platform as well.

As for hate speech, the Criminal Code of the Republic of Armenia provides punishment for acts of national, racial or religious hostility, racial superiority or degrading national dignity.[200] The aggravating circumstances for these acts are the following:

- the commission of these acts, whether publicly or through the use of mass media,
- the commission of these acts by using violence or threat of violence,
- using official position or commission of these acts by an organised group.[201]

The Criminal Code of Armenia provides punishment for the public calls for violence, public justification or propaganda of such violence based on gender, race, skin colour, ethnic or social origin, genetic background, language, religion, worldview, political or other views, national minority, property status, birth, disability, age or other personal or social circumstances[202] if there are no features of the crimes such as failure to actively comply with a lawful request by a government official during mass riots or calls for violence against persons,[203] acts of national, racial or religious hostility, racial superiority or degrading national dignity,[204] public calls for terrorism, terrorist financing and international terrorism, publicly justifying or propagating the commission of these crimes,[205] public calls to seize power, violate territorial integrity or forcibly overthrow constitutional order,[206] public calls for aggressive war,[207] the denial, mitigation, approval or justification of genocide and other crimes against peace and human security.[208] The aggravating circumstances provided by the Criminal Code for

200 Paragraph 1 of Article 226 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
201 Paragraph 2 of Article 226 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
202 Paragraph 1 of Article 226.2 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
203 The paragraph 4 of Article 225 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
204 Article 226 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
205 Article 226.1 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
206 Article 301 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
207 Article 385 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.
208 Article 397.1 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.

this provision, is the commission of these acts by a group of persons with prior consent or by an organized group or by using the official position.[209]

The RA legislation provides civil liability for harm to the honour, dignity and business reputation of a person through insult or defamation. But the hate speech may not contain insult or defamation. For example, if you come across an online post that calls for a minority to be deprived of their educational rights, these and other similar cases are certainly hate speech, but do not contain insult or defamation. Under Armenian law, insult is a public expression made to defame one's honour, dignity or business reputation through speech, image, voice, sign or otherwise and defamation is the public disclosure of a statement of fact that is untrue, and which discredits their honour, dignity or business reputation.

In the Republic of Armenia, it must be established civil liability by the law for online hate speech, which does not contain insult or defamation or the features of above-mentioned provisions of the Criminal Code of the RA. In such cases, a person must be able to apply the notice-to-notice system in order to get compensation and to demand to remove hate speech from online platforms.

One of the ways to solve this problem is the notice-and-takedown system. There are a lot of different opinions about this system. It allows an individual to apply to the online intermediary through which the hate speech is posted online, after which the latter removes that content.

The issue of hate speech and other illegal content online has generated controversy. It is accepted to think that the notice-and-takedown system is the most effective way to remove hate speech and illegal content online. Although intermediaries, hosts of Internet portals have all the technical means to remove the illegal content, that does not mean that the intermediaries can properly evaluate whether the content is illegal. It is preferable for an independent court to solve this issue, because intermediaries do not have the relevant experience to clarify such issues. Moreover, many intermediaries may have their own interest in removing illegal content. In this case, the person, who is the author of the illegal content does not have the opportunity to defend their rights. They can prove that the content is not illegal and does not contain hate speech at all. The suggestion that intermediaries should be responsible for the illegal content ignores the fact that the intermediaries only provide a platform and opportunity for the dissemination of ideas, opinions, but has nothing to do with that illegal content. Finally, removing the content from platforms by intermediaries not

[209] The paragraph 2 of Article 226.2 of Law No. 528 dated 1 August 2003, the Criminal Code of the RA.

only profoundly affects the right to freedom of expression on the internet, but also allows them to interfere with the privacy of their users and clients.

According to Article 19 - a British human rights organisation with a special mandate to protect and promote freedom of expression and freedom of information throughout the world: 'Intermediaries should not be responsible for any illegal comment. In addition, the State should not allow intermediaries to censor the Internet. This method can also overburden the judicial system, as there will be a lot of complaints, if we take into account the variety of opportunities to express yourself online. It will also be costly'.[210]

There is also another method of solving this issue, which will be effective in the RA as well. It is the method of notice-to-notice system. In this case, an individual or a group of people, who detect hate speech or illegal content, gets the opportunity to send a complaint to an intermediary that contains information about the illegal content, the person who posted it, the information that identify the person who posted it, the date and the time when the anti-legal content was installed. After this, the intermediary sends the complaint to the person, who allegedly committed the act, notifying the applicant as well. It is necessary to determine by the law how long it takes for the intermediary to send the complaint. 24 hours are enough for the intermediary to notify about the complaint to the alleged perpetrator. In addition, it is necessary to determine the cases, when the person who installed the illegal content, is unknown. It may be established by the law, that if it is impossible to find information for the identification of the alleged perpetrator, the accused person will be considered as unknown, and the victim can apply to the court and demand the removal and the refutation of hate speech or other illegal content. After this, the alleged person is able to remove the illegal content or to counteract it within a specified time (for example within 12 hours). This counterclaim must be transmitted to the applicant by the intermediary, after which the applicant will decide whether to appeal to the court or not. If the installer of the hate speech is unknown or refuses to disclose the identity, the applicant may apply to the court to detect the alleged person, to bring to civil liability and to remove the illegal content. It should be noted that the notice-to-notice system and civil responsibility should be applied to hate speech that does not contain insult or defamation. In the cases of serious crimes, religious, racial, or national grounds, the issue of responsibility must be solved by the Criminal Code of the Republic of Armenia.

[210] Intermediary liability: The debate (2013), page 14 <https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf> accessed 27 May 2020.

The Civil Code of the Republic of Armenia must also establish that if it is impossible to disclose the alleged perpetrator, the intermediary will be subject to civil liability only if it does not take any measures to remove the hate speech from the Internet. In this case, if we talk about hate speech that does not contain insult or defamation, the applicant should be able to apply to the court and bring the intermediary to civil responsibility, if it refuses to remove the illegal content.

These methods that include a notice-to-notice system will fill the gaps in the field of protection against hate speech on the Internet, in copyright etc. in the Republic of Armenia.

Summarising the above mentioned, we come to the conclusion that the right to freedom of expression should not be absolute on the platform as well: what is illegal in the offline domain is also illegal in the online domain. The Republic of Armenia has a lot of gaps in this sphere, but the methods outlined above will solve the issues without violating the right to freedom of expression.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

In Armenia the freedom of expression is guaranteed by Article 42 of the Constitution of the Republic of Armenia. In accordance with paragraph 1 of Article 42 of the Constitution everyone shall have the right to freely express their opinion, have own opinion, as well as to seek, receive and disseminate information and ideas through any media, without the interference of state or local self-government bodies and regardless of state frontiers.[211] As already stated, Armenian legislation does not literally distinguish online and offline legal relations, hence, the right to freedom of expression stated in the 42th Article of the Constitution of Armenia correspondingly refers to freedom of expression on the internet.

Paragraph 3 of Article 42 of the Constitution stipulates the retractable and limitable character of the freedom of expression. According to paragraph 3 of Article 42 of the Constitution any restrictions against the freedom of expression must be implemented only by law, for the purpose of state security, protecting public order, health and morals or the dignity and good reputation of others and other basic rights and freedoms thereof. [212]Indeed, any restriction against the

[211] Paragraph 1 of Article 42 of the Constitution of the Republic of Armenia 2015.
[212] Paragraph 3 of Article 42 of the Constitution of the Republic of Armenia 2015.

freedom of expression must comply with the principles of proportionality and certainty.[213] The following constitutional Article can be interpreted as a balancing tool between freedom of expression and protection of other rights and goods.

The Right to freedom of expression can be collided with the inviolability of private and family life, honour and good reputation codified in Article 31 of the Constitution of the Republic of Armenia. According to paragraph 1 of Article 31 of the Constitution right to inviolability of private and family life, honour and good reputation is guaranteed for everyone.[214] The inviolability of private and family life, honour and good reputation is not an absolute and unrestrictable and according to paragraph 2 of Article 31 of the Constitution may be restricted only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others.[215] The limitable character of both rights for the protection of the basic rights and freedoms of others can be interpreted as balance between aforementioned rights. Still, there are some elements such as the method of obtaining the information and its veracity, scale of the famousness of the person, content, which need to be taken into account. Details are to be regulated by case law. Though, both right to freedom of expression and inviolability of private and family life, honour and good reputation require equal respect.

The right to freedom of expression can collide with the right of protection of personal data under Article 34 of the Constitution of Armenia. According to Article 34 of the Constitution everyone shall have the right to data protection concerning them, get familiar with the data concerning them, request correction of any inaccurate data concerning them, as well as the right to the elimination of data obtained illegally or no longer having legal grounds.[216] Paragraph 4 of Article 34 of Article enables restrictions of the right to protection of personal data for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others.[217]

Further balance is not regulated by Armenian legislation. Collision between the right to freedom of expression, which includes right to receive and impart information, and the right of intellectual property is not excluded. According to paragraph 7 of Article 60 of the Constitution intellectual property shall be

213 Articles 78 and 79 of the Constitution of the Republic of Armenia 2015.
214 Paragraph 1 of Article 31 of the Constitution of the Republic of Armenia 2015.
215 Paragraph 2 of Article 31 of the Constitution of the Republic of Armenia 2015.
216 Article 34 of the Constitution of the Republic of Armenia 2015.
217 Paragraph 4 of Article 34 of the Constitution of the Republic of Armenia 2015.

protected by law.[218] The balance between these two rights could be generated through the cases of criminal conviction for copyright infringements in courts. Copyright infringements are regulated in the Law of the Republic of Armenia on Copyright and Related Rights. [219]

The right to freedom of expression could also violate human dignity of another person, which is, inviolable. according to Article 23 of the Constitution.[220]

Citizens of the Republic of Armenia have the right to apply to court in defence of their violated rights in the manner prescribed by law in case of violation of all the above-mentioned rights. Balancing the colliding rights, mainly, is finalized during the process of litigation.

It is noteworthy that freedom of expression does not qualify 'hate speech'. Council of Europe's Committee of Ministers defines 'hate speech' as a covering all form of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.[221] Currently the Standing Committee on State and Legal Affairs of the National Assembly of the Republic of Armenia tends to specify the legal regulations related to the word hate speech.[222]

The Republic of Armenia reached a minimum balance between allowing freedom of expression online and protecting other rights. The creation and implementation of more specific laws will be able to improve the existing balance between allowing freedom of expression online and protection of other rights.

---

218 Paragraph 7 of Article 60 of the Constitution of the Republic of Armenia 2015.

219 ՀՕ-142-Ն, Law of the Republic of Armenia on Copyright and Related Rights.

220 Article 23b of the Constitution of the Republic of Armenia 2015.

221 Council of Europe, Freedom of expression and information <https://www.coe.int/en/web/freedom-expression/freedom-of-expression-and-information-explanatory-memo> accessed 29 July 2020.

222 The Armenian Times, Hate speech is not freedom of speech <http://www.armtimes.com/hy/article/181620> accessed 29 July 2020.

10. How do you rank the access to freedom of expression online in your country?

Ranking - 4

The ranking is 4, because Armenia is not among the countries which exercise outrageous Internet restriction, there are not blocked social media, websites, pro-government commentators, arrested users (Freedom House Report 2018)[223] but, however, there are problems with Internet harassment, cyberbullying, violations of freedom of expression, low protection of personal data and some of these problems remain unanswered by Armenian legislation and practice.

Recent developments in Armenian reality has shown that one of the main problems regarding the freedom of expression online is its violations and hate speech.

Article 226 of the Criminal Code of Armenia criminalizes the actions which incite national, racial or religious hatred, racial supremacy or humiliation of national dignity. The problem with this Article is that it refers to only *actions* and does not cover the speech or propaganda of hatred, so it can be stated that hate speech is not criminalised in Armenia.

In Armenia the main platform of online discussions is Facebook and it is not uncommon to spread hate speech on this platform. One of the examples can be the wave of hatred and insults during the discussions of ratifications of the Convention on preventing and combating violence against women and domestic violence and the Convention on the protection of children against sexual exploitation and sexual abuse.

In 2019 Pink Armenia published a research on Hate speech displayed by State officials towards LGBT people in Armenia.[224] In the research it is demonstrated that online platforms are the main means of hate speech diffusion.

Victim shaming/blaming is also quite common in online platforms, especially towards female victims and the victims of domestic violence.[225]

Thus, the main problems in regard to the freedom of expression online in Armenia are hate speech and other violations of the freedom of expression.

---

223 Freedom House Report 2018 <https://freedomhouse.org/country/armenia/freedom-net/2018> accessed 29 July 2020.

224 Pink Armenia, Hate speech displayed by State officials towards LGBT people in Armenia <https://www.pinkarmenia.org/wpcontent/uploads/2019/05/hatespeech_en.pdf>.

225 The Armenian Weekly, Domestic Violence in Armenia: An Ugly Crime Still Denied <https://armenianweekly.com/2014/09/25/domestic-violence-armenia-ugly-crime-still-denied/> accessed 29 July 2020.

11. How do you overall assess the legal situation in your country regarding internet censorship?

Even though some legislative regulations exist which provide general protection of rights in this sphere, some problems still remain unaddressed by responsible authorities. For example, there are neither any regulations nor any policy papers or proposals in the Armenian legislation for future regulation of the issue of blocking and takedown of internet content. However, the legislation has systematically been improved during recent years and some positive changes ad stronger legal guarantees are expected.

Conclusion

The creation and implementation of more specific laws will make it possible to improve the existing balance between allowing freedom of expression online and protection of other rights. However, the Republic of Armenia has reached minimum balance between allowing freedom of expression online and protecting other rights.

The Republic of Armenia has some legislative gaps in this sphere, but the methods outlined in the report will lead us to the solution of the issues without violating the right to freedom of expression.

Table of legislation

Provision in Armenian language	**Corresponding translation in English**
ՀՀ Սահմանադրություն, հոդված 3 Մարդը, նրա արժանապատվությունը, հիմնական իրավունքները և ազատությունները 1. Հայաստանի Հանրապետությունում մարդը բարձրագույն արժեք է: Մարդու անօտարելի արժանապատվությունն իր իրավունքների և ազատությունների անքակտելի հիմքն է: 2. Մարդու և քաղաքացու հիմնական իրավունքների և ազատությունների հարգումն ու պաշտպանությունը հանրային իշխանության պարտականություններն են: 3. Հանրային իշխանությունը սահմանափակված է մարդու և քաղաքացու հիմնական իրավունքներով և ազատություններով՝ որպես անմիջականորեն գործող իրավունք:	Constitution of the RA, Article 3: The Human Being, His or Her Dignity, Basic Rights and Freedoms 1. The human being shall be the highest value in the Republic of Armenia. The inalienable dignity of the human being shall constitute the integral basis of his or her rights and freedoms. 2. The respect for and protection of the basic rights and freedoms of the human being and the citizen shall be the duty of the public power. 3. The public power shall be restricted by the basic rights and freedoms of the human being and the citizen as a directly applicable law.
ՀՀ Սահմանադրություն, հոդված 41 Մտքի, խղճի և կրոնի ազատությունը 1. Յուրաքանչյուր ոք ունի մտքի, խղճի, կրոնի ազատության իրավունք: Այս իրավունքը ներառում է կրոնը կամ համոզմունքները փոխելու ազատությունը և դրանք ինչպես միայնակ, այնպես էլ այլոց հետ համատեղ և հրապարակավ կամ մասնավոր կարգով՝ քարոզի, եկեղեցական արարողությունների, պաշտամունքի այլ ծիսակատարությունների կամ այլ ձևերով արտահայտելու ազատությունը: 2. Մտքի, խղճի և կրոնի ազատության արտահայտումը կարող է	**Constitution of the RA, Article 41:** **Freedom of Thought, Conscience and Religion** 1. Everyone shall have the right to freedom of thought, conscience and religion. This right shall include the freedom to change religion or belief and, either alone or in community with others and in public or in private, the freedom to manifest them in preaching, church ceremonies, other rites of worship or in other forms. 2. The expression of freedom of thought, conscience and religion may be restricted only by law for the purpose of state security, protecting public order, health and morals or the basic rights and freedoms of others.

սահմանափակվել միայն օրենքով՝ պետական անվտանգության, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով: 3. Յուրաքանչյուր քաղաքացի, որի կրոնական դավանանքին կամ համոզմունքներին հակասում է զինվորական ծառայությունը, ունի օրենքով սահմանված կարգով այն այլընտրանքային ծառայությամբ փոխարինելու իրավունք: 4. Կրոնական կազմակերպություններն իրավահավասար են և օժտված են ինքնավարությամբ: Կրոնական կազմակերպությունների ստեղծման և գործունեության կարգը սահմանվում է օրենքով:	3. Every citizen shall have the right to replace military service with alternative service, as prescribed by law, if it contradicts the religious faith or belief thereof. 4. Religious organisations shall enjoy legal equality and shall be vested with autonomy. The procedure for the establishment and operation of religious organisations shall be prescribed by law.
ՀՀ Սահմանադրություն, հոդված 42 Կարծիքի արտահայտման ազատությունը 1. Յուրաքանչյուր ոք ունի իր կարծիքն ազատ արտահայտելու իրավունք: Այս իրավունքը ներառում է սեփական կարծիք ունենալու, ինչպես նաև առանց պետական և տեղական ինքնակառավարման մարմինների միջամտության և անկախ պետական սահմաններից՝ տեղեկատվության որևէ միջոցով տեղեկություններ ու գաղափարներ փնտրելու, ստանալու և տարածելու ազատությունը: 2. Մամուլի, ռադիոյի, հեռուստատեսության և տեղեկատվական այլ միջոցների ազատությունը երաշխավորվում է: Պետությունը երաշխավորում է տեղեկատվական, կրթական, մշակութային և ժամանցային բնույթի հաղորդումների բազմազանություն առաջարկող անկախ հանրային	Constitution of the RA, Article 42: Freedom of Expression of Opinion 1. Everyone shall have the right to freely express his or her opinion. This right shall include freedom to hold own opinion, as well as to seek, receive and disseminate information and ideas through any media, without the interference of state or local self-government bodies and regardless of state frontiers. 2. The freedom of the press, radio, television and other means of information shall be guaranteed. The State shall guarantee the activities of independent public television and radio offering diversity of informational, educational, cultural and entertainment programmes. 3. Freedom of expression of opinion may be restricted only by law, for the purpose of state security, protecting public order, health and morals or the honour and good

հեռուստատեսության և ռադիոյի գործունեությունը: 3. Կարծիքի արտահայտման ազատությունը կարող է սահմանափակվել միայն օրենքով՝ պետական անվտանգության, հասարակական կարգի, առողջության և բարոյականության կամ այլոց պատվի ու բարի համբավի և այլ հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով:	reputation of others and other basic rights and freedoms thereof.
ՀՀ Սահմանադրություն, հոդված 76. Հիմնական իրավունքների և ազատությունների սահմանափակումներն արտակարգ կամ ռազմական դրության ժամանակ Արտակարգ կամ ռազմական դրության ժամանակ մարդու և քաղաքացու հիմնական իրավունքները և ազատությունները, բացառությամբ Սահմանադրության 23-26-րդ, 28-30-րդ, 35-37-րդ հոդվածներում, 38-րդ հոդվածի 1-ին մասում, 41-րդ հոդվածի 1-ին մասում, 47-րդ հոդվածի 1-ին մասում, 5-րդ մասի 1-ին նախադասությունում և 8-րդ մասում, 52-րդ, 55-րդ հոդվածի 2-րդ մասում, 56-րդ, 61-րդ, 63-72-րդ հոդվածներում նշվածների, կարող են օրենքով սահմանված կարգով ժամանակավորապես կասեցվել կամ լրացուցիչ սահմանափակումների ենթարկվել միայն այնքանով, որքանով դա պահանջում է իրավիճակը՝ արտակարգ կամ ռազմական դրության ժամանակ պարտավորություններից շեղվելու վերաբերյալ ստանձնված միջազգային պարտավորությունների շրջանակներում:	Constitution of the RA, Article 76 Restrictions on Basic Rights and Freedoms During State of Emergency or Martial Law During state of emergency or martial law, basic rights and freedoms of the human being and the citizen — with the exception of those referred to in Articles 23-26, 28-30, 35-37, part 1 of Article 38, part 1 of Article 41, part 1, first sentence of part 5 and part 8 of Article 47, Article 52, part 2 of Article 55, Article 56, Article 61, Articles 63-72 of the Constitution — may be temporarily suspended or subjected to additional restrictions under the procedure prescribed by law, only to the extent required by the existing situation within the framework of international commitments undertaken with respect to derogations from obligations during state of emergency or martial law.

ՀՀ Սահմանադրություն, հոդված 81 Հիմնական իրավունքներն ու ազատությունները և միջազգային իրավական պրակտիկան 1. Հիմնական իրավունքների և ազատությունների վերաբերյալ Սահմանադրությունում ամրագրված դրույթներ մեկնաբանելիս հաշվի է առնվում Հայաստանի Հանրապետության վավերացրած՝ մարդու իրավունքների վերաբերյալ միջազգային պայմանագրերի հիման վրա գործող մարմինների պրակտիկան: 2. Հիմնական իրավունքների և ազատությունների սահմանափակումները չեն կարող գերազանցել Հայաստանի Հանրապետության միջազգային պայմանագրերով սահմանված սահմանափակումները:	Constitution of the RA, Article 81 Basic Rights and Freedoms and International Legal Practice 1. The practice of bodies operating on the basis of international treaties on human rights, ratified by the Republic of Armenia, shall be taken into account when interpreting the provisions concerning basic rights and freedoms enshrined in the Constitution. 2. Restrictions on basic rights and freedoms may not exceed the restrictions prescribed by international treaties of the Republic of Armenia.
ՀՀ զանգվածային լրատվության մասին օրենք, հոդված 7 Լրատվության ոլորտում խոսքի ազատության իրավունքի սահմանափակումները 1. Արգելվում է օրենքով սահմանված կարգով գաղտնի համարվող կամ քրեորեն պատժելի արարքներ քարոզող, ինչպես նաև այնպիսի տեղեկատվության տարածումը, որը խախտում է մարդու անձնական և ընտանեկան կյանքի անձեռնմխելիությունը: 2. Արգելվում է տեսաձայնագրմամբ ստացված տեղեկատվության տարածումը, եթե դա ստացվել է տեսաձայնագրման կատարման մասին առանց անձին զգուշացնելու, և այդ անձն ակնկալել է, որ գտնվում է տեսաձայնագրումը կատարողի տեսադաշտից դուրս, լսելի չէ նրա համար և դրա համար ձեռնարկել է բավարար միջոցներ, բացառությամբ, երբ տեսաձայնագրումը կատարած	The Law of the RA on Media, Article 7: Restrictions of the freedom of speech in the sphere of mass media 1. It is prohibited to disseminate secret information as stipulated by law, or information advocating criminally punishable acts, as well as information violating the right to privacy of ones' personal or family life. 2. It is prohibited to disseminate information obtained by video and audio recording conducted without notifying the person of the fact or recording, when the person expected to be out of sight or earshot of the implementer of video and audio recording and has taken sufficient measures to ensure it, with the exception of situations when such measures were obviously not sufficient. 3. The dissemination of information related to one's personal or family life as well as those mentioned in the second part of this Article is allowed if it is necessary for the protection of public interest.

անձի տեսադաշտից դուրս լինելու կամ նրա համար լսելի չլինելու համար ձեռնարկված միջոցներն ակնհայտորեն անբավարար են եղել: 3. Սույն հոդվածի 2-րդ մասում նշված, ինչպես նաև մարդու անձնական և ընտանեկան կյանքին վերաբերող տեղեկատվության տարածումը թույլատրվում է, եթե դա անհրաժեշտ է հանրային շահերի պաշտպանության համար:	
ՀՀ հեռուստատեսության և ռադիոյի մասին օրենք, հոդված 22 Հեռուստառադիոհաղորդումների չարաշահման անթույլատրելիությունը 1. Արգելվում է հեռուստառադիոհաղորդումներն օգտագործել՝ 1) իշխանությունը բռնի զավթելու, Հայաստանի Հանրապետության սահմանադրական կարգը բռնությամբ փոխելու և տապալելու քարոզչության, 2) ազգային, ռասայական և կրոնական թշնամանք կամ երկպառակություններ սերմանելու, 3) պատերազմ քարոզելու, 4) քրեորեն պատժելի կամ գործող օրենսդրությամբ արգելված արարքների կոչեր տարածելու, 5) պոռնկագրություն տարածելու, 6) բռնության և դաժանության պաշտամունք պարունակող կամ քարոզող հաղորդումներ հեռարձակելու նպատակներով: Բացառություն կարող են լինել պատմափաստավավերագրական նյութերի օգտագործումն ու ցուցադրումը: 2. Էրոտիկ բնույթի հեռուստառադիոհաղորդումները և սարսափ ու ակնհայտ բռնություն պարունակող ֆիլմերը, ինչպես նաև անչափահասների առողջության,	The Law of the RA on Television and Radio Broadcasting, Article 22: The inadmissibility of abusing television and radio programs 1. It is forbidden to use television and radio programs for the following: 1) The campaign to seize authority by force, to forcibly change and overthrow the constitutional order of the Republic of Armenia 2) To disseminate national, racial and religious enmity or faction, 3) To advocate war, 4) To disseminate calls for criminal acts or acts prohibited by the current legislation, 5) To spread pornography, 6) For the purpose of broadcasting programs that contain or propagate a cult of violence and cruelty. Exceptions may be the use and display of historical documents. 2. Erotic television programs and films containing horror and obvious violence, such as programs that have a potentially negative impact on the health, mental and physical development and nurture of minors, except the subscription of broadcasting, can be broadcasted from 24.00-6.00 a.m.. The criteria for determining such programs is defined by the law.

մտավոր և ֆիզիկական զարգացման, դաստիարակության վրա հնարավոր բացասական ազդեցություն ունեցող հաղորդումները, բացառությամբ բաժանորդային հեռարձակման, կարող են ետեր հեռարձակվել ժամը 24.00-6.00-ն: Նման հաղորդումների որոշման չափորոշիչները սահմանվում են օրենքով: 3. Պետության կողմից հայտարարված սգո օրերին գովազդի և զվարճալի հաղորդումների հեռարձակումը հեռուստառադիոընկերությունների կողմից արգելվում է:	3. On the mourning days announced by the State, the broadcasting of commercials and entertaining programs by television and radio companies is prohibited.
Քաղաքացիական և քաղաքական իրավունքների մասին միջազգային դաշնագիր, հոդված 19 1. Յուրաքանչյուր մարդ իրավունք ունի անարգել կերպով հավատարիմ մնալ իր կարծիքներին: 2. Յուրաքանչյուր մարդ ունի իր կարծիքն ազատ արտահայտելու իրավունք. այդ իրավունքն ընդգրկում է, անկախ պետական սահմաններից, բանավոր, գրավոր կամ մամուլի միջոցով կամ էլ գեղարվեստական ձևով արտահայտված կամ մի այլ ձևով սեփական ընտրությամբ ամեն տեսակի ինֆորմացիա ու գաղափարներ որոնելու, ստանալու և տարածելու ազատությունը: 3. Սույն հոդվածի 2-րդ կետում նախատեսված իրավունքներից օգտվելը դնում է հատուկ պարտականություններ և հատուկ պատասխանատվություն: Հետևաբար, այն կապված է որոշ սահմանափակումների հետ, սակայն, պետք է սահմանվեն օրենքով և լինեն անհրաժեշտ. ա/ այլ անձանց իրավունքներն ու հեղինակությունը հարգելու համար.	International Covenant on Civil and Political Rights (ICCPR) Article 19 1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

բ/ պետական անվտանգության, հասարակական կարգի, բնակչության առողջության կամ բարոյականության պահպանության համար:	
Մարդու իրավունքների և հիմնական ազատությունների պաշտպանության մասին կոնվենցիա, հոդված 10 Արտահայտվելու ազատություն 1. Յուրաքանչյուր ոք ունի ազատորեն արտահայտվելու իրավունք: Այս իրավունքը ներառում է սեփական կարծիք ունենալու, տեղեկություններ և գաղափարներ ստանալու և տարածելու ազատությունը՝ առանց պետական մարմինների միջամտության և անկախ սահմաններից: Այս հոդվածը չի խոչընդոտում պետություններին՝ սահմանելու ռադիոհաղորդումների, հեռուստատեսային կամ կինեմատոգրաֆիական ձեռնարկությունների լիցենզավորում: 2. Այս ազատությունների իրականացումը, քանի որ այն կապված է պարտավորությունների և պատասխանատվության հետ, կարող է պայմանավորվել այնպիսի ձևականություններով, պայմաններով, սահմանափակումներով կամ պատժամիջոցներով, որոնք նախատեսված են օրենքով և անհրաժեշտ են ժողովրդավարական հասարակությունում՝ ի շահ պետական անվտանգության, տարածքային ամբողջականության կամ հասարակության անվտանգության, անկարգությունները կամ հանցագործությունները կանխելու, առողջությունը կամ բարոյականությունը, ինչպես և այլ անձանց հեղինակությունը կամ իրավունքները պաշտպանելու, խորհրդապահական պայմաններով	European Convention on Human Rights, Article 10: Freedom of expression 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

ստացված տեղեկատվության բացահայտումը կանխելու կամ արդարադատության հեղինակությունն ու անաչառությունը պահպանելու նպատակով:	
ՀՀ Սահմանադրություն, հոդված 31 Մասնավոր և ընտանեկան կյանքի, պատվի ու բարի համբավի անձեռնմխելիությունը 1. Յուրաքանչյուր ոք ունի իր մասնավոր և ընտանեկան կյանքի, պատվի ու բարի համբավի անձեռնմխելիության իրավունք: 2. Մասնավոր և ընտանեկան կյանքի անձեռնմխելիության իրավունքը կարող է սահմանափակվել միայն օրենքով՝ պետական անվտանգության, երկրի տնտեսական բարեկեցության, հանցագործությունների կանխման կամ բացահայտման, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով:	Constitution of the RA, Article 31: Inviolability of Private and Family Life, Honour and Good Reputation 1. Everyone shall have the right to inviolability of his or her private and family life, honour and good reputation. 2. The right to inviolability of private and family life may be restricted only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others.
ՀՀ Սահմանադրություն, հոդված 34 Անձնական տվյալների պաշտպանությունը 1. Յուրաքանչյուր ոք ունի իրեն վերաբերող տվյալների պաշտպանության իրավունք: 2. Անձնական տվյալների մշակումը պետք է կատարվի բարեխղճորեն, օրենքով սահմանված նպատակով, անձի համաձայնությամբ կամ առանց այդ համաձայնության՝ օրենքով սահմանված այլ իրավաչափ հիմքի առկայությամբ: 3. Յուրաքանչյուր ոք իրավունք ունի ծանոթանալու պետական և տեղական ինքնակառավարման մարմիններում	Constitution of the RA, Article 34: Protection of Personal Data 1. Everyone shall have the right to protection of data concerning him or her. 2. The processing of personal data shall be carried out in good faith, for the purpose prescribed by law, with the consent of the person concerned or without such consent in case there exists another legitimate ground prescribed by law. 3. Everyone shall have the right to get familiar with the data concerning him or her collected at state and local self-government bodies and the right to request correction of any inaccurate data

իր մասին հավաքված տվյալներին և պահանջելու ոչ հավաստի տվյալների շտկում, ինչպես նաև ապօրինի ձեռք բերված կամ այլևս իրավական հիմքեր չունեցող տվյալների վերացում: 4. Անձնական տվյալներին ծանոթանալու իրավունքը կարող է սահմանափակվել միայն օրենքով՝ պետական անվտանգության, երկրի տնտեսական բարեկեցության, հանցագործությունների կանխման կամ բացահայտման, հասարակական կարգի, առողջության և բարոյականության կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով: 5. Անձնական տվյալների պաշտպանությանը վերաբերող մանրամասները սահմանվում են օրենքով:	concerning him or her, as well as elimination of data obtained illegally or no longer having legal grounds. 4. The right to get familiar with personal data may be restricted only by law, for the purpose of state security, economic welfare of the country, preventing or disclosing crimes, protecting public order, health and morals or the basic rights and freedoms of others. 5. Details related to the protection of personal data shall be prescribed by law.
ՀՀ Սահմանադրություն, հոդված 23 Մարդու արժանապատվությունը Մարդու արժանապատվությունն անխախտելի է:	Constitution of the RA, Article 23: Human Dignity Human dignity is inviolable
ՀՀ Սահմանադրություն, հոդված 60 Սեփականության իրավունքը 1. Յուրաքանչյուր ոք ունի օրինական հիմքով ձեռք բերած սեփականությունն իր հայեցողությամբ տիրապետելու, օգտագործելու և տնօրինելու իրավունք: 2. Ժառանգելու իրավունքը երաշխավորվում է: 3. Սեփականության իրավունքը կարող է սահմանափակվել միայն օրենքով՝ հանրության շահերի կամ այլոց հիմնական իրավունքների և	Constitution of the RA, Article 60: Right of Ownership 1. Everyone shall have the right to possess, use and dispose of legally acquired property at his or her discretion. 2. The right to inherit shall be guaranteed. 3. The right of ownership may be restricted only by law, for the purpose of protecting public interests or the basic rights and freedoms of others. 4. No one may be deprived of ownership except through judicial procedure, in the cases prescribed by law. 5. Alienation of property with a view to ensuring overriding public interests shall be carried out in exceptional cases and under

ազատությունների պաշտպանության նպատակով: 4. Ոչ ոք չի կարող զրկվել սեփականությունից, բացառությամբ դատական կարգով՝ օրենքով սահմանված դեպքերի: 5. Հանրության գերակա շահերի ապահովման նպատակով սեփականության օտարումն իրականացվում է օրենքով սահմանված բացառիկ դեպքերում և կարգով՝ միայն նախնական և համարժեք փոխհատուցմամբ: 6. Հողի սեփականության իրավունքից չեն օգտվում օտարերկրյա քաղաքացիները և քաղաքացիություն չունեցող անձինք, բացառությամբ օրենքով սահմանված դեպքերի: 7. Մտավոր սեփականությունը պաշտպանվում է օրենքով: 8. Յուրաքանչյուր ոք պարտավոր է մուծել օրենքին համապատասխան սահմանված հարկեր, տուրքեր, կատարել պետական կամ համայնքային բյուջե մուտքագրվող պարտադիր այլ վճարումներ:	the procedure prescribed by law, only with prior and equivalent compensation. 6. Foreign citizens and stateless persons shall not enjoy the right of ownership over land, except for the cases prescribed by law. 7. Intellectual property shall be protected by law. 8. Everyone shall be obliged to pay taxes and duties prescribed in accordance with law and make other mandatory payments to the state or community budget.
ՀՀ Սահմանադրություն, հոդված 51 Տեղեկություններ ստանալու իրավունքը 1. Յուրաքանչյուր ոք ունի պետական և տեղական ինքնակառավարման մարմինների ու պաշտոնատար անձանց գործունեության մասին տեղեկություններ ստանալու և փաստաթղթերին ծանոթանալու իրավունք: 2. Տեղեկություններ ստանալու իրավունքը կարող է սահմանափակվել միայն օրենքով՝ հանրային շահերի կամ այլոց հիմնական իրավունքների և ազատությունների պաշտպանության նպատակով:	Constitution of the RA Article 51 The right of receiving information 1. Everyone shall have the right to receive information and get familiar with documents relating to the activities of State and local self-government bodies and officials. 2. The right to receive information may be restricted only by law, for the purpose of protecting public interests or basic rights and freedoms of others. 3. The procedure for receiving information, as well as the grounds for liability of officials for concealing information or for unjustified refusal of

3. Տեղեկություններ ստանալու կարգը, ինչպես նաև տեղեկությունները թաքցնելու կամ դրանց տրամադրումն անհիմն մերժելու համար պաշտոնատար անձանց պատասխանատվության հիմքերը սահմանվում են օրենքով:	providing information thereby shall be prescribed by law.
ՀՀ Սահմանադրություն, հոդված 43 Ստեղծագործության ազատությունը Յուրաքանչյուր ոք ունի գրական, գեղարվեստական, գիտական և տեխնիկական ստեղծագործության ազատություն:	Constitution of the RA Article 43 The freedom of creation Everyone shall have the freedom of literary, artistic, scientific and technical creation.
ՀՀ Քաղաքացիական օրենսգիրք, հոդված 1087.1, մաս 10 Պատվին, արժանապատվությանը կամ գործարար համբավին պատճառված վնասի հատուցման կարգը և պայմանները Անձը չի կարող օգտվել սույն հոդվածի 7-րդ և 8-րդ կետերով սահմանված պաշտպանության միջոցներից, եթե նա մինչև դատարան դիմելը «Զանգվածային լրատվության մասին» Հայաստանի Հանրապետության օրենքով սահմանված կարգով պահանջել է հերքում և (կամ) իր պատասխանի հրապարակում, և լրատվական գործունեություն իրականացնողը կատարել է այդ պահանջը:	Civil Code of RA, Article 1087.1, Paragraph 10 Procedure for and conditions of compensation for the damage caused to honour, dignity or business reputation The person may not benefit from the means of protection defined in points 7 and 8 of this Article, where he or she, before applying to court, has required refutation and/or publication of the response thereof as prescribed by the Law of the Republic of Armenia 'On mass media', and the entity carrying out media activities has complied with that request.
ՀՀ Քաղաքացիական օրենսգիրք, հոդված 3, մաս 1 և մաս 2	Civil Code of RA, Article 3, Section 1 and section 2 Principles of civil legislation

Քաղաքացիական օրենսդրության սկզբունքները 1. Քաղաքացիական օրենսդրությունը հիմնվում է իր կողմից կարգավորվող հարաբերությունների մասնակիցների հավասարության, կամքի ինքնավարության և գույքային ինքնուրույնության, սեփականության անձեռնմխելիության, պայմանագրի ազատության, մասնավոր գործերին որևէ մեկի կամայական միջամտության անթույլատրելիության, քաղաքացիական իրավունքների անարգել իրականացման անհրաժեշտության, խախտված իրավունքների վերականգնման ապահովման, դրանց դատական պաշտպանության սկզբունքների վրա: 2. Քաղաքացիները և իրավաբանական անձինք քաղաքացիական իրավունքները ձեռք են բերում ու իրականացնում իրենց կամքով և ի շահ իրենց: Նրանք ազատ են պայմանագրի հիման վրա սահմանելու իրենց իրավունքները և պարտականությունները, որոշելու պայմանագրի՝ օրենսդրությանը չհակասող ցանկացած պայման:	1. Civil legislation is based on the principles of equality, autonomy of will, and property autonomy of the participants of relations regulated thereby, inviolability of ownership, freedom of contract, impermissibility of arbitrary interference by anyone in private affairs, necessity of unhindered exercise of civil rights, ensuring the reinstatement of violated rights, judicial protection thereof. 2. Citizens and legal persons shall acquire and exercise civil rights upon their will and to their benefit. They shall be free in the establishment of their rights and responsibilities on the basis of a contract, in determining any condition of the contract not contradicting with the legislation. Civil rights may be restricted only by law, where it is necessary for the purposes of protection of state and public security, public order, health and morals of the public, rights and freedoms, honour and good reputation of others.
ՀՀ Քաղաքացիական օրենսգիրք, հոդված 11 Քաղաքացիական իրավունքների իրականացումը 1. Քաղաքացիները և իրավաբանական անձինք իրենց պատկանող քաղաքացիական իրավունքները՝ ներառյալ դրանց պաշտպանության իրավունքը, իրականացնում են իրենց հայեցողությամբ: 2. Քաղաքացիների և իրավաբանական անձանց հրաժարվելն իրենց իրավունքներն իրականացնելուց չի հանգեցնում այդ իրավունքների	Civil Code of the Republic of Armenia Article 11 Exercise of civil rights 1. Citizens and legal persons shall at their discretion exercise the civil rights belonging thereto, including the right of protection thereof. 2. Renunciation by citizens and legal persons to exercise their rights shall not entail termination of these rights, except for the cases provided for by law.

դադարման, բացառությամբ օրենքով նախատեսված դեպքերի:	
ՀՀ Քաղաքացիական օրենսգիրք, հոդված 19 Պատվի, արժանապատվության, գործարար համբավի պաշտպանությունը 1. Անձի պատիվը, արժանապատվությունը, գործարար համբավը ենթակա են պաշտպանության այլ անձի կողմից հրապարակայնորեն արտահայտված վիրավորանքից և զրպարտությունից՝ սույն օրենսգրքով և այլ օրենքներով սահմանված դեպքերում ու կարգով: 2. Քաղաքացու պատվի և արժանապատվության պաշտպանությունը շահագրգիռ անձանց պահանջով թույլատրվում է նաև նրա մահից հետո: 3. Եթե անձի պատիվը, արժանապատվությունը կամ գործարար համբավն արատավորող տեղեկությունները տարածած անձին պարզելն անհնար է, ապա անձը, ում մասին նման տեղեկություններ են տարածվել, իրավունք ունի դիմելու դատարան՝ տարածված տեղեկություններն իրականությանը չհամապատասխանող ճանաչելու պահանջով:	Civil Code of RA, Article 19 Protection of honour, dignity and business reputation 1. Honour, dignity and business reputation shall be protected from insult and slander publicly expressed by other person in the cases and under the procedure provided for by this Code and other laws. 2. The protection of the honour and dignity of a citizen may, upon the request of interested parties, be permitted also following his or her death. 3. In case of impossibility of identifying the person who has disseminated information disgracing a person's honour, dignity or business reputation, the person in respect of which such information was disseminated shall have the right to apply to court with a request of declaring the disseminated information as not corresponding to the reality.
ՀՀ Քաղաքացիական օրենսգիրք, հոդված 162 Ոչ նյութական բարիքների հասկացությունը 1. Անձի կյանքը և առողջությունը, արժանապատվությունը, անձնական անձեռնմխելիությունը, պատիվն ու բարի անունը, գործարար համբավը, մասնավոր կյանքի անձեռնմխելիությունը, անձնական ու	Civil Code of RA, Article 162 Concept of intangible assets 1. Life and health, dignity, personal inviolability, honour and good name, business reputation, inviolability of private life, privacy of personal and family life, the right of freedom of movement, of choice of the place of residence and location, right to one's name, right of authorship and other personal non-property rights and

ընտանեկան կյանքի գաղտնիությունը, ազատ տեղաշարժվելու, բնակվելու և գտնվելու վայր ընտրելու իրավունքը, անվան իրավունքը, հեղինակության իրավունքն ու քաղաքացուն ի ծնե կամ օրենքի ուժով պատկանող այլ անձնական ոչ գույքային իրավունքները և ոչ նյութական բարիքներն անօտարելի են ու անփոխանցելի: Օրենքով նախատեսված դեպքերում ու կարգով անձնական ոչ գույքային իրավունքները և այլ ոչ նյութական բարիքները, որոնք պատկանել են մահացածին, կարող են իրականացվել ու պաշտպանվել այլ անձանց՝ ներառյալ իրավատիրոջ ժառանգների կողմից: 2. Ոչ նյութական բարիքները, սույն օրենսգրքին և այլ օրենքներին համապատասխան, պաշտպանվում են դրանցով նախատեսված դեպքերում ու կարգով, ինչպես նաև այն դեպքերում ու այն սահմաններում, որոնցում քաղաքացիական իրավունքների պաշտպանության եղանակների օգտագործումը (հոդված 14) բխում է խախտված ոչ նյութական իրավունքի էությունից և այդ խախտումների հետևանքների բնույթից:	intangible assets belonging to a citizen from birth or by virtue of law are inalienable and non-transferable. In cases and in the manner provided for by law, personal nonpropert rights and other intangible assets belonging to a deceased person may be exercised and protected by other persons, including heirs of the rightholder. 2. Intangible assets shall be protected in accordance with this Code and other laws in cases and in the manner provided for thereby, as well as in those cases and within those limits in which the use of the ways of protection of civil rights (Article 14) follows from the essence of the violated intangible right and the nature of the consequences of this violation.
ՀՀ Քաղաքացիական օրենսգիրք, հոդված 14 Քաղաքացիական իրավունքների պաշտպանության եղանակները Քաղաքացիական իրավունքների պաշտպանությունն իրականացվում է՝ 1) իրավունքը ճանաչելով. 2) մինչև իրավունքի խախտումը եղած դրությունը վերականգնելով. 3) իրավունքը խախտող կամ դրա խախտման համար վտանգ ստեղծող գործողությունները կանխելով.	Civil Code of RA, Article 14. Ways of protection of civil rights Protection of civil rights shall be carried out through: (1) recognition of the right; (2) restoration of the situation having existed before the violation of the right; (3) prevention of actions violating the right or creating a threat for the violation thereof; (4) applying the consequences of the invalidity of a void transaction;

4) առոչինչ գործարքի անվավերության հետևանքները կիրառելով. 5) վիճահարույց գործարքն անվավեր ճանաչելով և դրա անվավերության հետևանքները կիրառելով. 6) պետական կամ տեղական ինքնակառավարման մարմնի ակտն անվավեր ճանաչելով 7) դատարանի կողմից պետական և տեղական ինքնակառավարման մարմնի՝ օրենքին հակասող ակտը չկիրառելով. 8) իրավունքի ինքնապաշտպանությամբ. 9) պարտականությունը բնեղենով կատարելուն հարկադրելով. 10) վնասներ հատուցելով 11) տուժանք բռնագանձելով. 12)իրավահարաբերությունը դադարեցնելով կամ փոփոխելով. 13) օրենքով նախատեսված այլ եղանակներով:	(5) declaring a disputable transaction as invalid and applying the consequences of the invalidity thereof; (6) declaring an act of a state or local self-government body as invalid; (7) not applying by the court of the act of a state and local self-government body that contradicts the law; (8) self-protection of the right; (9) enforcing the performance of the duty in kind; (10) compensation for damages; (11) levy a default penalty; (12) termination or alteration of a legal relation; (13) other ways provided for by law.
«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, հոդված 3, մաս 1, կետ 10 և կետ 11 1. Սույն օրենքում օգտագործվում են հետևյալ հիմնական հասկացությունները. 10) անձնական տվյալների ուղեփակում՝ անձնական տվյալները հավաքելու կամ ամրագրելու կամ համակարգելու կամ փոխանցելու կամ օգտագործելու հնարավորության ժամանակավոր կասեցում. 11) անձնական տվյալների ոչնչացում՝ գործողություն, որի արդյունքում հնարավոր չէ վերականգնել.	RA law on Protection of Personal Data Article 3, section 1, subsection 10 and subsection 11 1. The following main concepts shall be used in this Law: (…); (10) blocking of personal data - temporary suspension of the possibility to collect or fix or systematise or transfer or use personal data; (11) destruction of personal data - an operation, which renders the restoration of the content of personal data contained in an information system impossible.

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, հոդված 5 Համաչափության սկզբունքը 1. Տվյալների մշակումը պետք է հետապնդի օրինական նպատակ, դրան հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ և չափավոր: 2. Անձնական տվյալներ մշակողը պարտավոր է անձնական տվյալները մշակել այն նվազագույն քանակով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար: 3. Արգելվում է այնպիսի անձնական տվյալների մշակումը, որոնք անհրաժեշտ չեն տվյալները մշակելու նպատակի համար կամ անհամատեղելի են դրա հետ: 4. Արգելվում է անձնական տվյալների մշակումը, եթե տվյալները մշակելու նպատակին հնարավոր է հասնել ապանձնավորված կերպով: 5. Անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար:	RA law on Protection of Personal Data Article 5 Principle of proportionality 1. The processing of data must pursue a legitimate purpose, measures to achieve it must be suitable, necessary and moderate. 2. The processor of personal data shall be obliged to process the minimum volume of personal data that are necessary for achieving legitimate purposes. 3. The processing of personal data that are not necessary for the purpose of processing of data or are incompatible with it shall be prohibited. 4. The processing of personal data shall be prohibited where the purpose of processing of data is possible to achieve in a depersonalised manner. 5. Personal data must be stored in such a way as to exclude the identification thereof with the data subject for a period longer than is necessary for achieving predetermined purposes.
«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, հոդված 6 Հավաստիության սկզբունքը 1. Մշակվող անձնական տվյալը պետք է լինի ամբողջական, ճշգրիտ, պարզ և հնարավորինս թարմացված:	RA law on Protection of Personal Data, Article 6 Principle of reliability 1. The personal data being processed must be complete, accurate, simple and, where necessary, kept up to date.

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, հոդված 7 Սուբյեկտների նվազագույն ներգրավման սկզբունքը 1. Անձնական տվյալների մշակումն իրականացվում է սուբյեկտների նվազագույն ներգրավման սկզբունքով: 2. Այն դեպքում, երբ պետական կառավարման կամ տեղական ինքնակառավարման մարմինը, նոտարը միասնական էլեկտրոնային տեղեկատվական համակարգի միջոցով կարող են անձնական տվյալը ձեռք բերել այլ մարմնից, ապա անձնական տվյալների սուբյեկտից չի պահանջվում ներկայացնել որոշակի գործողությունների համար անհրաժեշտ անձնական տվյալը: 3. Անձնական տվյալների սուբյեկտի գրավոր համաձայնության դեպքում անձնական տվյալներ մշակող համարվող ֆիզիկական կամ իրավաբանական անձինք կարող են պետական կամ տեղական ինքնակառավարման մարմնից ստանալ որոշակի գործողության համար անհրաժեշտ և անձնական տվյալների սուբյեկտի գրավոր համաձայնության մեջ ուղղակիորեն մատնանշված անձնական տվյալը: 4. Էլեկտրոնային տեղեկատվական համակարգի միջոցով անձնական տվյալների փոխանցման կարգը սահմանում է Հայաստանի Հանրապետության կառավարությունը:	RA law on Protection of Personal Data Article 7 Principle of minimum engagement of subjects 1. The processing of personal data shall be carried out under the principle of minimum engagement of subjects. 2. Where the state administration or local self-government body, the notary are able to obtain the personal data from other body through a uniform electronic information system, personal data subject shall not be required to submit personal data necessary for certain operations. 3. In case of a written consent of the personal data subject, natural or legal persons considered as a processor of personal data may obtain from a state or local self-government body personal data necessary for a certain operation and directly specified in the written consent of a personal data subject. 4. The procedure for the transfer of personal data through an electronic information system shall be prescribed by the Government of the Republic of Armenia.
«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, հոդված 8 Անձնական տվյալները մշակելու օրինականությունը	RA law on Protection of Personal Data Article 8 Lawfulness of processing personal data

1. Անձնական տվյալներ մշակելը օրինական է, եթե՝ 1) տվյալները մշակվել են օրենքի պահանջների պահպանմամբ, և տվյալների սուբյեկտը տվել է իր համաձայնությունը, բացառությամբ սույն օրենքով կամ այլ օրենքներով ուղղակիորեն նախատեսված դեպքերի, կամ 2) մշակվող տվյալները ձեռք են բերվել անձնական տվյալների հանրամատչելի աղբյուրներից:	1. The processing of personal data shall be lawful, where: (1) the data have been processed in observance of the requirements of the law and the data subject has given his or her consent, except for cases directly provided for by this Law or other laws; or (2) the data being processed have been obtained from publicly available sources of personal data.
«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, հոդված 15, մաս 1 և մաս 2 Տվյալների սուբյեկտի՝ իր անձնական տվյալների վերաբերյալ տեղեկություններ ստանալու իրավունքը 1. Տվյալների սուբյեկտն իրավունք ունի ստանալու տեղեկություններ իր անձնական տվյալների, տվյալները մշակելու, մշակելու հիմքերի և նպատակների, տվյալները մշակողի, նրա գտնվելու վայրի մասին, ինչպես նաև այն անձանց շրջանակի մասին, որոնց կարող են փոխանցվել անձնական տվյալները: 2. Տվյալների սուբյեկտն իրավունք ունի ծանոթանալու իր անձնական տվյալներին, մշակողից պահանջելու ուղղել, ուղեփակել կամ ոչնչացնել իր անձնական տվյալները, եթե անձնական տվյալներն ամբողջական կամ ճշգրիտ չեն կամ հնացած են կամ ձեռք են բերվել անօրինական ճանապարհով կամ անհրաժեշտ չեն մշակելու նպատակներին հասնելու համար:	RA law on Protection of Personal Data Article 15, section 1 and section 2 Right of data subject to information on his or her personal data 1. The data subject shall have the right to information on his or her personal data, processing of data, grounds and purposes for processing, processor of data, the registered office thereof, as well as the scope of persons to whom personal data may be transferred. 2. The data subject shall have the right to get familiarised with his or her personal data, require from the processor to rectify, block or destruct his or her personal data, where the personal data are not complete or accurate or are outdated or has been obtained unlawfully or are not necessary for achieving the purposes of the processing.
«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենք, հոդված 16	RA law on Protection of Personal Data, Article 16

Տվյալների սուբյեկտի իրավունքները անձնական տվյալները մշակելու հիման վրա որոշումներ ընդունելիս 1. Արգելվում է անձնական տվյալներ մշակելու նպատակներից չբխող այնպիսի որոշումներ ընդունել, որոնք տվյալների սուբյեկտի համար առաջացնում են իրավական հետևանքներ կամ այլ կերպ առնչվում են նրա իրավունքներին ու օրինական շահերին, բացառությամբ սույն հոդվածի 2-րդ մասով նախատեսված դեպքերի: 2. Անձնական տվյալները մշակելու հիման վրա տվյալների սուբյեկտի համար իրավական հետևանքներ առաջացնող կամ այլ կերպ նրա իրավունքներին ու օրինական շահերին առնչվող որոշումներն ընդունվում են տվյալների սուբյեկտի համաձայնությամբ կամ օրենքով նախատեսված դեպքերում:	Rights of data subject when delivering decisions based on processing personal data 1. It shall be prohibited to deliver decisions not stemming from the purposes of processing personal data, which give rise to legal consequences for the data subject or otherwise affect his or her rights and legitimate interests, except for cases provided for by part 2 of this Article. 2. Decisions giving rise to legal consequences for the data subject or otherwise affecting his or her rights and legitimate interests based on processing of personal data may be delivered by the data subject's consent or in cases provided for by law.
«Էլեկտրոնային հաղորդակցության մասին» ՀՀ օրենք, հոդված 2 Սույն օրենքում օգտագործվող հասկացությունները Սույն օրենքում օգտագործվող հիմնական հասկացություններն ունեն հետևյալ իմաստները՝ (…). ծառայություններ մատուցող՝ Կարգավորողի կողմից լիազորված կամ Կարգավորողին սույն օրենքի համաձայն ծանուցում ներկայացրած ցանկացած անձ, որն առաջարկում է հանրային էլեկտրոնային հաղորդակցության ծառայություններ. (…). օպերատոր՝ ցանկացած անձ, որը Կարգավորողի կողմից լիազորված է տիրապետել և շահագործել հանրային էլեկտրոնային հաղորդակցության ցանցը՝ էլեկտրոնային	RA law on Electronic Communications Article 2 Concepts used in this Law The main concepts used in this Law have the following meaning: (…); 'Internet service provider' – a person that provides an Internet access service; (…); 'Operator' – any person authorised by the Regulator to hold and operate a public electronic communications network for the purpose of providing electronic communications services. When providing services over its network, an operator shall be treated as a service provider; (…).

հաղորդակցության ծառայություններ մատուցելու նպատակով: Իր ցանցով ծառայություններ մատուցելու դեպքում օպերատորը համարվում է ծառայություններ մատուցող. (…):	
«Էլեկտրոնային հաղորդկցության մասին» ՀՀ օրենք, հոդված 50 Միջամտություն, ձայնագրում կամ հաղորդագրությունների բացահայտում 1. Էլեկտրոնային հաղորդակցության ցանկացած միջոցով փոխանցվող հաղորդագրության կողմ չհանդիսացող որևէ անձ կարող է միջամտել, ձայնագրել հաղորդագրությունը կամ բացահայտել դրա պարունակությունը միայն տվյալ հաղորդագրության կողմերի գրավոր համաձայնությամբ կամ դատարանի որոշմամբ՝ օրենքով նախատեսված դեպքերում և կարգով: 2. Ի լրումն սույն հոդվածի առաջին մասի դրույթների, հանրային կամ մասնավոր էլեկտրոնային հաղորդակցության ցանցերի օպերատորները և հանրային կամ մասնավոր էլեկտրոնային ծառայություններ մատուցողները կամ նրանց աշխատակիցներն ու ներկայացուցիչները կարող են միջամտել կամ վերահասցեագրել հաղորդագրությունները կամ ազդանշանները՝ չբացահայտելով դրանք, եթե այդ միջամտությունը կամ ազդանշաններ վերահասցեագրելը պայմանավորված է վերջիններիս աշխատանքային պարտականությունների իրականացմամբ: 3. Օրենքով նախատեսված դեպքերում և կարգով բոլոր օպերատորները և ծառայություն մատուցողները պարտավոր են ապահովել իրավապահ և ազգային անվտանգության	RA law on Electronic Communications Article 50 Interception, recording, or disclosure of messages 1. A person other than a party to a message transmitted by any electronic communications means may intercept, record, or disclose the content of such message only upon the written consent of the parties to the message or upon a court order in cases and in the manner provided for by law. 2. In addition to the provisions of part 1 of this Article, operators of public or private electronic communications networks and providers of public or private electronic services as well as their employees or representatives may intercept or redirect messages or signals, without disclosing them where such interception or redirection of signals is conditioned by the exercise of their official duties. 3. In cases and in the manner provided for by law, all operators and service providers shall be obliged to provide access to law enforcement and national security personnel to any communications equipment, facilities, switches, routers, or other similar equipment, including wiretapping devices.

աշխատակիցների մուտքը հաղորդակցության սարքավորումներին, ենթակառուցվածքներին, միացնող-անջատող, ուղղորդող և նմանատիպ այլ սարքերին, ներառյալ՝ գաղտնալսումների իրականացման համար անհրաժեշտ սարքերին:	
«Էլեկտրոնային հաղորդակցության մասին» ՀՀ օրենք Հոդված 51. Ծառայության կամ ենթակառուցվածքների ոչ պատշաճ օգտագործումը Օպերատորը կամ ծառայություններ մատուցողը, որը գիտակցաբար թույլ է տալիս, որպեսզի իր ցանցը կամ ծառայություններն օգտագործվեն որևէ անձի կողմից այլ անձանց խաբեության ենթարկելու, նրանց նկատմամբ բռնություն, չարամտություն, սպառնալիքներ կամ շանտաժ կիրառելու նպատակով, ենթարկվում է սույն օրենքի 63-րդ հոդվածով նախատեսված տույժի, որը չպետք է գերազանցի հինգ միլիոն դրամը:	RA Law on Electronic Communications Article 51 Improper usage of services or infrastructures An operator or service provider who knowingly permits its network or service to be used by a person to deceive, to employ violence, to expose malignity, threaten, or intimidate any other person shall be subject to a penalty provided for by Article 63 of this Law, which shall not exceed five million drams.
«Արտակարգ դրության իրավական ռեժիմի մասին» ՀՀ օրենք, հոդված 10, մաս 1 և մաս 2 Արտակարգ դրության պայմաններում ժամանակավոր սահմանափակումների և կիրառվող միջոցների սահմանները 1. Սույն օրենքում նշված իրավունքների և ազատությունների նկատմամբ սույն օրենքով թույլատրվող սահմանափակումները պետք է կիրառվեն բացառապես այն նպատակներով, որոնց համար նախատեսվել են, և պետք է լինեն համաչափ՝ հիշյալ նպատակների համեմատությամբ: 2. Արտակարգ դրության պայմաններում գործադիր	RA law on Legal Regime of the State of Emergency Article 10, section 1 and section 2 Borders of temporary limitations and used means during the state of emergency 1. Limitations to the rights and freedoms, set up in the Law, shall be exercised exceptionally for the goals, for which they are provided, and shall be proportional to them. 2. In course of the state emergency the actions of executive bodies shall be compatible with the situation for which the state of emergency has been declared.

իշխանության մարմինների գործողությունները պետք է համարժեք լինեն արտակարգ դրություն հայտարարելու համար հիմք ծառայած հանգամանքներով պայմանավորված իրավիճակին:	
ՀՀ Քրեական դատավարության օրենսգիրք, հոդված 278 Դատական վերահսկողության ոլորտը 1. Դատարանը քննում է քննչական, օպերատիվ-հետախուզական գործողություններ կատարելու և անձի հիմնական իրավունքները և ազատությունները սահմանափակող դատավարական հարկադրանքի միջոցներ կիրառելու վերաբերյալ միջնորդությունները: 2. Դատարանը, սույն օրենսգրքով սահմանված դեպքերում և կարգով, քննում է հետաքննության մարմինների, քննիչի, դատախազի և օպերատիվ-հետախուզական գործունեություն իրականացնող մարմինների որոշումների և գործողությունների օրինականության վերաբերյալ բողոքները: 3. Դատարանի՝ սույն հոդվածի առաջին մասով նախատեսված դեպքերում ընդունվող որոշումները կարող են վերանայվել վերադաս դատարանի կողմից՝ դատախազի, միջնորդություն հարուցած մարմնի, այն անձանց կամ նրանց ներկայացուցիչների բողոքի հիման վրա, որոնց շահերը շոշափվում են:	Criminal Procedure Code of the RA Article 278 Domain of court supervision The court considers the implementation of investigative, operative and searching activities and the petitions concerning the application of judiciary enforcement restricting the constitutional rights and freedoms of the person. The court considers complaints concerning the legitimacy of decrees and actions of preliminary investigation bodies, investigators, prosecutors and operative and searching bodies in accordance with the procedure specified in this Code. The court decrees mentioned in part 1 of this Article can be reconsidered by the higher court, based on the petition of a body concerning the actions of the prosecutor, and the complaint of the persons or their representatives whose interests were affected.
«Վարչարարության հիմունքների և վարչական վարույթի մասին» ՀՀ օրենք, հոդված 4 Վարչարարության օրինականությունը 1. Վարչական մարմինները պարտավոր են հետևել օրենքների պահպանմանը:	The Law on Fundamentals of Administration and Administrative Procedure Article 4 Legality of administrative action 1. Administrative bodies shall ensure the observance of the laws.

2. Վարչական մարմինների լիազորությունները սահմանվում են օրենքով կամ օրենքով նախատեսված դեպքերում՝ իրավական այլ ակտերով:	2. The powers of administrative bodies shall be laid down by law or, in cases envisaged by law, other legal acts.
«Վարչարարության հիմունքների և վարչական վարույթի մասին» ՀՀ օրենք, հոդված 6 Հայեցողական լիազորությունները սահմանափակելը 1. Հայեցողական լիազորությունն օրենքով վարչական մարմնին վերապահված իրավունք է՝ ընտրելու մի քանի հնարավոր իրավաչափ լուծումներից որևէ մեկը: 2. Հայեցողական լիազորություն իրականացնելիս վարչական մարմինը պարտավոր է առաջնորդվել մարդու և քաղաքացու՝ Հայաստանի Հանրապետության Սահմանադրությամբ ամրագրված իրավունքների և ազատությունների պաշտպանության անհրաժեշտությամբ, նրանց իրավահավասարության, վարչարարության իրականացման համաչափության և կամայականության արգելքի սկզբունքներով, ինչպես նաև հետապնդել օրենքով կանխորոշված այլ նպատակներ:	The Law on Fundamentals of Administration and Administrative Procedure Article 6 Restriction of discretionary powers 1. Discretionary power is a right granted to an administrative body by law to choose one of several possible legitimate solutions. 2. In the exercise of discretionary power administrative body shall be guided by the necessity to protect human and citizens' rights and freedoms prescribed by the Constitution of the Republic of Armenia, their equality, the principles of proportionality of administration and prohibition of arbitrariness, as well as pursue other goals prescribed by law.
«Վարչարարության հիմունքների և վարչական վարույթի մասին» ՀՀ օրենք, հոդված 7 Կամայականության արգելքը 1. Վարչական մարմիններին արգելվում է անհավասար մոտեցում ցուցաբերել միատեսակ փաստական հանգամանքների նկատմամբ, եթե առկա չէ դրանց տարբերակման որևէ հիմք: Վարչական մարմինները պարտավոր են անհատական մոտեցում	The Law on Fundamentals of Administration and Administrative Procedure Article 7 Prohibition of arbitrariness 1. Administrative bodies shall be prohibited from manifesting unequal treatment towards the similar factual circumstances, unless there is any grounds for their differentiation.

ցուցաբերել էապես տարբեր փաստական հանգամանքների նկատմամբ: 2. Եթե վարչական մարմինը որևէ հայեցողական լիազորություն իրականացրել է որոշակի ձևով, ապա միանման դեպքերում հետագայում ևս պարտավոր է իր այդ հայեցողական լիազորությունն իրականացնել նույն ձևով: Վարչական մարմինն այդ սահմանափակումից կարող է հրաժարվել, եթե գերակա շահի առկայության պատճառով նա հետագայում մտադիր է մշտապես ընդունել մեկ այլ հայեցողական որոշում:	Administrative bodies are obliged to manifest individualized treatment towards essentially different factual circumstances. 2. If the administrative body has exercised its discretionary power in a certain manner, then in similar cases in the future it is obliged to exercise the discretionary power in the same manner. Administrative body may derogate from that restriction if, on the grounds of supervening interest, it intends to consistently adopt this other approach to the exercise of its discretion.
«Վարչարարության հիմունքների և վարչական վարույթի մասին» ՀՀ օրենք, հոդված 8 Վարչարարության համաչափությունը Վարչարարությունը պետք է ուղղված լինի Հայաստանի Հանրապետության Սահմանադրությամբ և օրենքներով հետապնդվող նպատակին, և դրան հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ և չափավոր:	The Law on Fundamentals of Administration and Administrative Procedure, article 8 Proportionality of administrative action Administrative action must be directed at an objective pursued under the Constitution and laws of the Republic of Armenia, and the measures for achieving that objective must be suitable, necessary and proportional.
«Վարչարարության հիմունքների և վարչական վարույթի մասին» ՀՀ օրենք, հոդված 11 Տնտեսավարությունը Վարչական մարմինն իր լիազորություններն իրականացնելիս պարտավոր է գործել այնպես, որպեսզի առանց իր լիազորությունների կատարմանը վնասելու՝ առավել սեղմ ժամկետում, առավել բարենպաստ արդյունքի հասնելու համար ապահովի իր տնօրինմանը հանձնված միջոցների	The Law on Fundamentals of Administration and Administrative Procedure, article 11 Efficient Operation In the exercise of its powers, an administrative body shall act so that it secures the maximally efficient use of the means at its disposal for in such a manner as to, without undermining the performance of its powers, ensure the most effective utilisation of means submitted to its

առավել արդյունավետ օգտագործումը:	disposal, in shortest possible term and for assuring the most faviourable results.
«Հեղինակային իրավունքի և հարակից իրավունքների մասին» ՀՀ օրենք, հոդված 22.1, մաս 1 և մաս 2 Լրատվական նյութի օգտագործման պայմանները 1. Տպագիր լրատվական միջոցների, էլեկտրոնային կայքերի (ցանցային լրատվության միջոց) լրատվական նյութերից քաղվածքների վերարտադրումը այլ տպագիր լրատվական միջոցներում, ինտերնետային կայքերում թույլատրվում է իրականացնել միայն մեջբերման նպատակն արդարացնող ծավալով՝ առանց հեղինակի (հեղինակային իրավունքի իրավատիրոջ) համաձայնության և վարձատրության վճարման: Անկախ վերարտադրման ծավալից՝ լրատվական նյութերից քաղվածքների վերարտադրումը չպետք է բացահայտի լրատվական նյութի էական մասը: (…): Լրատվական նյութի ամբողջական վերարտադրումը կարող է իրականացվել միայն հեղինակի (հեղինակային իրավունքի իրավատիրոջ) համաձայնության դեպքում: (…): 2. Տպագիր լրատվական միջոցներում, էլեկտրոնային կայքերում այլ տպագիր լրատվական միջոցների, էլեկտրոնային կայքերի լրատվական նյութերից քաղվածքներ վերարտադրելիս պետք է հղում կատարել լրատվական նյութի սկզբնաղբյուրին: (…):	RA law on Copyright and Related Rights Article 22.1, section 1 and section 2 Conditions for using the news articles 1. Articles from printed media resources, websites (digital media resources) shall be expressed in other media resources, websites only to the extent is justified by the purpose of the quotation, without paying the author the fee to use the article. Regardless of the extent of quotations, it shall not express the essential part of the original article. (…). The article shall be fully implemented, provided that it has been agreed upon with the author of the article (…). 2. If articles from printed media resources, websites (digital media resources) shall be expressed in other media resources, mention shall be made of their initial source.

Bibliography

English titles

Legislation

Constitution of the Republic of Armenia

The Law on Mass Media of the Republic of Armenia

The Law on Television and Radio of the Republic of Armenia

The Law on Freedom of information

The Law on the libraries and the activity of libraries

The Law on protection of personal data

The Civil Code of the RA

International Covenant on Civil and Political Rights (ICCPR)

European Convention on Human Rights

The Law of the Republic of Armenia on Copyright and Related Rights

Criminal Code of Republic of Armenia

Criminal Procedure Code of the Republic of Armenia

The Law of the Republic of Armenia on Electronic Communications

The Law on Legal Regime of the State of Emergency

The Law on Compulsory Enforcement of Court Orders

The Law on Fundamentals of Administration and Administrative Procedure

Decision of the Government of the Republic of Armenia on Declaring a State of Emergency in the Republic of Armenia, N 298

Reports

Freedom House Report 2018

Hate speech displayed by State officials towards LGBT people in Armenia

Third Quarter Report by CPFE on Situation with Freedom of Expression and Violations of Rights of Journalists and Media in Armenia (2019)

Intermediary liability: the debate (2013),

UNGA (10 August 2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/66/290

Comparative study on blocking, filtering and take-down of illegal internet content, Lausanne, 20 December 2015

Books

The Online Media Self-Regulation Guidebook / Ed. by A. Hulin and M. Stone; Vienna: OSCE Representative on Freedom of the Media, 2013 – 110 page

Digital resources

www.ohchr.org

www.coe.int

www.freedomhouse.org

https://prwb.am

www.aravot.am

www.osce.org

www.armtimes.com

www.news.am

www.armenianweekly.com

http://www.concourt.am

https://iravaban.net

https://eur-lex.europa.eu

https://gdpr-info.eu

Case law

Couderc and Hachette Filipacchi Associés v France App no 40454/07 (ECHR, 10 November 2015).

Constitutional Court of the Republic of Armenia, Decision of 23 February 2016 No. SDV-1256.

Cassation Court of the Republic of Armenia, Decision of 27 April 2012, No. LD/0749/02/10.

Jersild v. Denmark., (Application no. 15890/89), judgement of September 23, 1998

Hertel v. Switzerland, (Application no. 25181/94), 25 August 1998

Steel and Morris v. the United Kingdom (Application no. 68416/01), February 15, 2005

Delfi AS v. Estonia, (Application no. 64569/09), judgement of 16 June 2015

Constitutional Court decision no. SDV-997 of 11 November 2011

Case of Artur Grigoryan v. 'Hraparak' daily newspaper LLC, First Instance Court of General Jurisdiction of Kentron and Nork-Marash districts, case no. EKD/2491/02/11 ('ԵԿԴ/2491/02/11'), 7th of March, 2012

ELSA Azerbaijan

Contributors

National Coordinator

Aytaj Mammadova

National Researchers

Sona Karimova

Lale Ahmadzada

Seljan Mammadli

Maya Ahmadzada

National Linguistic Editor

Nigar Hidayatzada

National Technical Editor

Aydan Abdullayeva

Introduction

The following part of the report addresses aspects of internet censorship in Azerbaijan, as well as other related issues such as freedom of expression, legislation on the issue of blocking or takedown of internet, 'right to be forgotten', 'right to delete,' rules governing orders towards internet intermediaries and cases when their liability arise. Generally, the state of internet or situation of online environment in Azerbaijan are among the priorities of this research. The Republic of Azerbaijan recently has made many progressive leaps for the purpose of catching up with developed countries on the internet sphere. Moreover, while discussing the condition of freedom of expression, freedom of internet and overall the status of internet in Azerbaijan, one should also consider the very short period of independence of Azerbaijan from the oppressed regime of the USSR and ongoing conflict between Azerbaijan and Armenia. Nagorno-Karabakh conflict makes the internet to be under the surveillance of the state in order to prevent the dissemination of fake news and any propagandas. In fact, almost all post-soviet countries in comparison to others have struggled a lot after dissolution of the USSR with regard to the previously mentioned internet issues.

Issues relating to the internet that will be explained exclusively in this article, are constituting the area of study of Informational Law in Azerbaijan, which is a complex branch of law covering almost all fields of law regulating social relations. That is why there is both specific legislation and other rules regulating the problems concerning informational law such as more importantly, relevant articles of Criminal Code, Civil Code, Administrative Code, Constitution of Azerbaijan, or other normative legal acts may be given as examples. Furthermore, while governing informational cases, International Law has a legal effect over them and because of mostly the universal character of informational-related circumstances. There is an obvious impact of informational law on preparing national legislation of this field and according to the Constitution of Azerbaijan, if there would be contradictions between national law and international law, except to the Constitution of acts adopted by referendum of Azerbaijan, international law prevails.

Nowadays, Azerbaijan is still on the way to improving itself on the internet sphere, which is inevitably a crucial element of the modern world, and in fact, sustainable development of the country automatically demands internet relations according growth. Day-by-day new State Programs are accepted such as 'The State Program on realizing the National Strategy on development of informational community in the Republic of Azerbaijan covering the years of

2016-2020'[226] is still continuing to accomplish its aims. Likewise, the programmes, the new additions to the Criminal Law, and recently accepted laws on regulating internet issues are also essential to think through and all of these endeavours are the indication of the future success of Azerbaijan in this field.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

Azerbaijan is bound by international laws to respect freedom of expression and related fundamental rights, including the right to freedom of assembly and association, and to ensure their protection.[227] Starting from these obligations, the Constitution of Azerbaijan and the local law of Azerbaijan contain many provisions on freedom of expression and other related rights. For example, Article 47 of the constitution guarantees freedom of thought and speech.[228] In addition, Article 50 stipulates that everyone has the right to distribute information, that freedom of the mass media is guaranteed, and that censorship is prohibited.[229]

Some of these include the protection of freedom of expression in accordance with international standards. But some provisions contradict the standards and cause great anxiety. These sections contain general information on the relevant local legislative framework in Azerbaijan, mainly provisions directly related to freedom of expression, as well as other laws sometimes used to suppress freedom of expression in the Azerbaijani environment.[230] Freedom of expression and freedom of information are protected under the Constitution of the Republic of Azerbaijan. Article 47 emphasises that 'freedom of thought and expression' and is said, 'No one shall be compelled to express his views or beliefs or to renounce his ideas and beliefs.'[231]

Article 50 states that 'Everyone has the right to seek, receive, transmit, prepare and impart information that everyone wants.'[232] Mass media, including the press, say state censorship is prohibited and freedom of mass media is guaranteed.

---

226 E-qanun.az <http://www.e-qanun.az/framework/33717> accessed 14 February 2020.
227 Alasgar Mammadli, Legal restrictions and responsibilities of freedom of expression, published on September 2017.
228 Article 47 of Constitution of the Republic of Azerbaijan (1999).
229 Article 50 of Constitution of the Republic of Azerbaijan (1999).
230 ibid.
231 Article 47 of the Constitution of the Republic of Azerbaijan (1999).
232 Article 50 of the Constitution of the Republic of Azerbaijan (1999).

Although everyone has the rights, freedoms, and inalienable rights of their birth from the moment of their birth, according to Article 24 of the Constitution, 'Rights and freedoms also include everyone's responsibility and responsibilities to society and others.'[233]

Parallel to the rights and freedoms, these articles also contain certain restrictions. Restrictions on freedom of expression are defined in Article 47 as these: incitement to racial hatred and hostility; inciting national hatred and hostility; inciting religious enmity and hostility; inciting social enmity and hostility; campaign and propaganda are not allowed. Restrictions on freedom of information are not explicitly stated in Article 50 of the Constitution, but merely 'the right to refute or respond to information published in the media', which violates the rights or interests of anyone. "It should be noted that this provision was included in Article 50 after the August 2009 referendum."[234]

Although the Constitution is not explicitly stated in its text, the constitutional law adopted by the Milli Majlis and intended to bring the exercise of Human Rights and Freedoms in the Republic of Azerbaijan to the European Convention on the Protection of Human Rights and Fundamental Freedoms restricts freedom of expression.[235] These are interests of state security; protection of health and morals, rights and freedoms of other persons; crime prevention; preventing disorders; protection of public safety; ensuring the interests of the territorial integrity of the state; protection of the authority or rights of other persons; prevent disclosure of confidential information; ensuring the reputation and impartiality of the court.[236]

The purpose of 'protection of the rights and dignity of other persons', which is one of the bases provided by the Constitutional Law, is stated in several articles in the Constitution itself. Article 32 of the Constitution guarantees the individual's right to personal immunity. The right to protection of honour and dignity as defined in Article 46 of the Constitution is also a constitutional right. These rights constitute red lines of restrictions on freedom of expression, freedom of information and freedom of the media.[237] Human rights and freedoms are mentioned in the Constitution as a whole. In addition to provisions that directly regulate freedom of expression, freedom of information and the media, these rights are also taken into account in the context of human rights

233 Article 24 of the Constitution of the Republic of Azerbaijan (1999).
234 Alasgar Mammadli, Legal restrictions and responsibilities of freedom of expression, published on September 2017.
235 ibid.
236 ibid.
237 ibid.

and freedoms. Article 71 further emphasizes that these rights, as well as the grounds for their restriction, are justified. According to the article, the legislative, executive and judicial authorities must maintain and protect the human and civil rights and freedoms enshrined in the Constitution.

Basically, there are no unlimited rights and freedoms. This has been taken into account and Article 71 provides that 'Everyone's rights and freedoms are limited by the constitution and laws as well as the rights and freedoms of others. No one can restrict the exercise of human and civil rights and freedoms.'[238]

In addition to the factors limiting the rights and freedoms outlined in the Constitution, there are also legal grounds. These bases derive their source from the interests enshrined in the Constitution and the Constitutional Law itself. One such law is the Law of the Republic of Azerbaijan 'On Mass Media'. Article 10 of the Media Law, which prohibits the use of freedom of mass media, states:

'… The use of the media to discredit citizens, honour or dignity, and to publish, slander, or commit any other wrongdoing is not permitted.'

Article 60 of this Law sets out the liability for the abuse of freedom of mass information. Editorial (responsible editor) of mass media and journalists (authors) bear civil, administrative, criminal and other liability in accordance with the legislation of the Republic of Azerbaijan in the following cases: when disclosure of information prohibited by law; if the editor-in-chief (editor) does not control the preparation of printed materials in accordance with the requirements of the Law on Mass Media; Distribution of information without reference to its source, except in cases provided by the Law on Mass Media; Attempt to the private life of citizens; publishing or issuing pornographic materials.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

The issue of blocking and takedown of internet content has been explicitly defined under the relevant legislative acts of the Republic of Azerbaijan such as 'Law on Mass Media', 'Law of the Republic of Azerbaijan on telecommunications', 'Law of the Republic of Azerbaijan on accession to the Charter and the Convention on the International Telecommunication Union, as well as the adjustment documents', 'The Law of Azerbaijan Republic on the right to obtain information', 'Law on Information, Informatization, and Protection of

238 Article 71 of the Constitution of the Republic of Azerbaijan (1999).

Information' etc., as well as appropriate parts of the Criminal Code and Civil Code of Azerbaijan. Circumstances leading blocking or takedown of internet content are constituting one of the parts of informational law. In Azerbaijan, informational law is not an independent sphere of law, because of the regulation mechanism of it. From this point of view, the informational law, as well as the grounds under which the internet content can be blocked or taken down as a component of it, can be adjusted not only by laws of Milli Majlis (Parliament) of Azerbaijan related to such a field of law. The Constitution of Azerbaijan, International Treaties to which the Republic of Azerbaijan is party, civil, criminal and administrative legislations, acts adopted by referendum, regulations of Constitutional and Supreme Courts of Azerbaijan, etc. can be taken into consideration while listing the legislation and sources of informational law and its components. 'Azerbaijan is a party to all major regional and international human rights treaties guaranteeing freedom of expression, including the ICCPR and the ECHR. Under Article 151 of the Constitution, international agreements binding upon Azerbaijan prevail over domestic legislation, with the exception of the Constitution itself and acts accepted by way of the referendum.'[239]

The Republic of Azerbaijan pays efficient attention to the development of means of regulation of information systems, internet protection and its sufficiency. During 2005-2008 the State Programme on the improvement of communication and information technologies was adopted, thus the main purpose of this programme was to establish 'Electron Azerbaijan'. Nowadays, Azerbaijan is a party to a number of international organisations and, accordingly most of their conventions. Since January 2001, Azerbaijan has co-operated with the members of the Council of Europe as its one of the member states. The Council of Europe adopted an action plan of 2018-2021 for the progress of Azerbaijan which encompasses almost every sphere, including informational development. Moreover, a significant amount of money for the construction and expansion of internet infrastructure in Azerbaijan has been collected from the State Oil Fund.

Freedom of information, freedom of expression through the internet, control over the internet, equality of the usage of internet, simplifying the access to the internet, all in all, the establishment of conditions for thriving all means of the internet community are under the supervision of government authorities. Thus, in some cases, restrictions can be put on internet contents, and even it can be removed to minimize the risk to society, protection, and establishment of law-abiding internet systems without any danger to the everyday life of people and

[239] National Framework for Internet Freedom in Azerbaijan (Baku, 2013), 6.

the state. Article 12 of the Constitution states that 'The highest priority objective of the state is to provide for the rights and freedoms of a person and citizen.'

One of the most important laws on this issue is 'Law on Mass Media' adoption of which by the Parliament of Azerbaijan dated back to July 1999. Additionally, another example is the 'Law of the Republic of Azerbaijan on telecommunications'[240] 'Law of the Republic of Azerbaijan on accession to the Charter and the Convention on the International Telecommunication Union, as well as the adjustment documents'[241] show opportunities to understand the international regulations on the issue of informational law, as well as the cases when the internet content may be blocked or taken down. Consequently, the scope of the last-mentioned law is wider than the 'Law of the Republic of Azerbaijan on telecommunications.' 'By adopting [this] law on May 14, 2000, the legislative organ of Azerbaijan, The Parliament (Milli Mejlis) recognized the application of international legal regulations in the country.'[242] 'The Law of Azerbaijan Republic on the right to obtain information' was adopted on 9 December 2005. '[This] law provided a starting point for the use of the Internet in the system of state administration.' Article 29 of this Law provides a list of information to be disclosed by information owners. In addition to the available tools, the government agencies must disclose the information specified in that list via the Internet as well. By stating in its Article 31 that 'If this obligation arises also based on requirements of Article 29.1 hereof, the public information is included in Internet Information Resources.'[243]

As will be mentioned in the next question of this article, the internet content is commonly blocked or taken down due to the political reasons for the aim of the ultimate goal of the state – promotion of peace and justice, as well as social order among the population and state security. According to Article 41 of the 'Law on Mass Media' for the breach of Article 3, 4, 34, 36 of this law the responsibility does occur. Moreover, new articles regarding this issue have been added in the text of the Criminal Code, in addition to the previous ones, within considering the ones in Civil Code. The perpetrator may be accused of the unlawful actions

---

240 Passed by the Azerbaijani Parliament (Milli Mejlis) on 14 June 2005 and came into force by the Decree of the President of the Republic of Azerbaijan No. 277 issued on 9 August 2005.

241 National Framework for Internet Freedom in Azerbaijan <https://www.irfs.org/wp-content/uploads/2014/01/National-Framework-for-Internet-Freedom-in-Azerbaijan.pdf> accessed 14 February 2020.

242 Cis-legislation: Law of the Azerbaijan Republic about Personal Data <https://cis-legislation.com/document.fwx?rgn=31412> last accessed 14 February 2020.

243 Law of the Republic of Azerbaijan on right to obtain information <http://www.commission-anticorruption.gov.az/upload/file/Law_on_right_to_obtain_information_done.pdf> last accessed 14 February 2020.

of him/her against cybersecurity based on both Civil and Criminal Codes if those actions have been prescribed in both of them as entailing criminal or civil responsibility. In November 2016, penalties were increased for online insult and libel. A new provision to Article 148(1) of the Criminal Code targeted insult or slander disseminated online by fake usernames or accounts. The increased penalties include a fine of AZN 1,000-1,500 (about US$590-885), community service for 360-480 hours, or corrective labour for up to one year.[244] The new penalties imposed include a fine of AZN 1,000-1,500, community service for 240-480 hours, corrective labour for up to one year, or imprisonment for up to six months. Article 147 of the Criminal Code targets the 'dissemination, in a public statement, publicly exhibited work of art, through the mass media or a publicly displayed Internet information resource, of knowingly false information discrediting the honour and dignity of a person or damaging his or her reputation.' The second part of this article states libel becomes punishable by corrective labour for a term of up to two years, or by imprisonment for a term of up to three years when it accuses someone 'of having committed a serious or especially serious crime.'[245]

In May 2017, changes to Article 323(1) of the Criminal Code introduced a maximum sentence of five years in prison for defaming or humiliating the honour and dignity of the president in mass media, which includes social media.[246] The fine also increased to AZN 1.500-2.500.[247] Thus, amendments approved in December 2017 impose fines on individuals, officials, and legal entities for disseminating banned content online.

The grounds for blocking internet content can be defamation through internet, arising national, religious or any other conflicts within the usage of internet, dissemination of children pornography, humiliation of Head of the Country, but not other governmental authorities, inducing buying or selling narcotic substances and other intoxicated psychotropic substances, and other actions constituting threats against state security and integrity. In March, the Parliament made amendments to the Law on Information, Informatisation, and Protection of Information. These amendments forbid the dissemination of some actions and reinforce the stated grounds for blocking or takedown of internet content.

244 Defamation and insult laws in the OSCE region: A comparative study, OSCE the Representatives of Freedom of the Media Dunja Mijatovic, March 2017, <https://www.osce.org/fom/303181?download=true> accessed 14 February 2020.

245 The criminal code of the republic of Azerbaijan, <http://www.e-qanun.az/code/11> accessed 14 February 2020.

246 Parliament adopted introduction of criminal liability for insulting the president online, Minval.az, November 29. 2016, <http://bit.ly/2qU9HmQ> accessed 14 February 2020.

247 The punishment for 'damaging' the President increased, Azadliq.org, May 31, 2017, <https://www.azadliq.org/a/28520698.html> accessed 14 February 2020.

It composes calls for terrorism, and information on methods and means of carrying out terrorist acts; religious hatred or hostility and explicit calls for the violation of territorial integrity, violent coup and organisation of mass riots.[248] The realisation of the rules derived from these amendments is conducted based on the following procedure:

'Amendments to the Law on Information, Informatisation, and Protection of Information passed in March 2017, compel website owners to take down "prohibited information" if warned by authorities. If the authorities deem that the content poses a danger to the state or society and the website owner fails to comply with the order within eight hours, a government representative can immediately block the website. This process was applied to the five websites ordered to be blocked in May 2017.'[249]

Azerbaijan signed the European Convention on Human Rights on 1 January 2001, and Parliament ratified it on 25 December 2001. It was ratified on 15 April 2002, which is considered as the date of the entry into the force of the Convention with regard to Azerbaijan.[250] Following the accession to the Convention, Azerbaijan also passed the Constitutional Law on Human Rights in 2002. This law starts with a provision that prohibits the abuse of rights and with a general prohibition of the violation of the rights of others.[251] Thus, this default rule, also forbids the violation of rights of others by any means, even throughout the internet.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

The Republic of Azerbaijan is a country in which freedom of expression, freedom of information and other fundamental human rights and freedoms are protected under the Constitution and of the country such as the law of the Parliament on Mass media of 7 December 1999, relevant chapters of Criminal Code and Civil Code of Azerbaijan, 'Law of the Republic of Azerbaijan "On access to information', 'Law of the Republic of Azerbaijan about information, informatisation, and information security', Law of the Republic of Azerbaijan 'On Personal Data' and so on. Under the Constitution of the Republic of

248 Mapping media freedom, Index on Censorship
< https://mappingmediafreedom.ushahidi.io/posts/21726> accessed 14 February 2020.

249 Report of Freedom House on Freedom on the Net 2018 in Azerbaijan,
<https://freedomhouse.org/report/freedom-net/2018/azerbaijan> accessed 14 February 2020.

250 Information on signing and ratification <http://conventions.coe.int> accessed 14 February 2020.

251 Article 148.2 of the Constitution.

Azerbaijan the fundamental rights and freedoms of man and citizen are; right to equality, right to life, right to liberty, right to property, right to intellectual property, and right to inviolability of private life, etc. The means of mass information and media in Azerbaijan shall conform with the constitutional requirements first which set the basic standards for the establishment of abiding internet content and information circulation. The usage and protection of information on the internet in Azerbaijan are very subtle problems. Additionally, State filtering and blockage of the internet are rarely confronted in the digital world of Azerbaijan because of a lack of political conflicts, defamation cases through the internet, and affinity of political opposition to the usage of other means to make an influence on their supporters rather than the internet. The international treaties and conventions having some sort of internet-related content and rules can also be applied in Azerbaijan, in consideration of the rules of the hierarchy of legislative acts prescribed in the Constitution of Azerbaijan.

As mentioned in the introduction part, internet content commonly can be blocked/filtered due to political controversies. Those can be related to both the manipulative information of opponents of the national government of Azerbaijan on the internet and the fake or humiliating information against the national security interests of Azerbaijan, especially in Armenian-Azerbaijan Nagorno-Karabakh conflict. For example, all Armenian internet sites have been blocked in Azerbaijan. Moreover, as the Republic of Azerbaijan is a democratic state and a country governed under the rule of law, taking down or blocking an internet content is not applied systematically as mentioned in the application of Freedom House dated back to 2014, unlike for in the People's Republic of China, Turkmenistan, Iran, Tajikistan, Pakistan and for other most of the Eastern countries. That is because Azerbaijan is one of the parties to the information community dissimilar to the third world countries or where democracy lacks its essence. The information community is composed of states in which the majority of their population can access the internet, can use it freely, lawfully, and process it without any discrimination or obstruction. In Azerbaijan, approximately, six million people out of the total population of 10 have preceding rights which paves a path for the bright technological and digital future of this country. Again, according to the application of Freedom House of 2014, internet in Azerbaijan is semi-free, so during the time of some struggles within the country, difficulties on access to the internet or reaching some internet content have arisen.

Grounds on which the internet content may be blocked/filtered or taken down/removed in Azerbaijan are stipulated under relevant legislation. Furthermore, the Civil Code, Criminal Code, and Administrative Code of

Azerbaijan may have the power to put accordingly, civil/criminal/administrative responsibility on similar issues as prescribed on their proper articles. One of the most important documents regulating internet content is the law of the Parliament on Mass media of 12 July 1999. According to Article 41 of this law, for the breach of Article 3, 4, 34, 36, the responsibility does occur. Article 3 is about the inadmissibility of censorship in Azerbaijan, and if the authoritative persons, state bodies, legal entities, organisations or parties and other public unions would violate the norms of this article, responsibility is automatically applied and the internet content regarding this violation is being blocked. Article 4 is about the unacceptability of misusing of means of mass media. Thus, usage of means of mass media for violation or dissemination of state secret and other secrets specifically protected under the law, extermination or changing of existing constitutional state and integrity of the country, propagating war, violence and cruelty or for creation of conflict in the sphere of national, religious, gender or ethnic identity, shall be entitled to responsibility. The internet content including these proscribed issues must be banned, blocked, or taken down from public access to protect the socially important values and interests of society and state.

Obscenity has been defined under Article 242 of the Criminal Code as 'unlawful manufacture for distribution or advertising, distribution, advertising of pornographic materials or items, as well as illegal trade in printed publications, film or video materials, images or other pornographic objects' with a fine in the amount of 2,000 to 4,000 AZN, or correctional labour for up to two years, or imprisonment for up to three years with or without deprivation of the right to hold a certain position or engage in certain activities for up to three years. Hate speech within obscenity can sometimes illegally be the essence of the internet content which obliges ultimate takedown of it. Article 283 of the Criminal Code prohibits 'incitement of national, racial, social or religious hatred and enmity'. Incitement can be understood as 'actions aimed at the incitement of national, racial, social or religious hatred and enmity, the humiliation of national dignity, as well as actions aimed at restricting the rights of citizens, or establishing the superiority of citizens based on their national, racial, or religious belonging if such acts are committed in public or through the use of mass media.' Such incitement is punishable with a fine from 1000 to 2000 AZN, or correctional labour for up to two years, or imprisonment from two to four years. However, if such incitement is committed 'with the use or threat of violence', 'by a person using an official position', or 'by an organised group', then incitement is punishable by imprisonment from three to five years. Alongside incitement and obscenity, unlawful distribution of private, confidential and secret information

is one of the grounds to remove the internet content if it contains such illegality. Criminal Code provides in Article 156 ('Infringement of inviolability of private life') that 'illegal collection, dissemination of information about the private life of a person that constitutes his personal or family secret, as well as the sale or transfer to another person of documents, video and photo materials, sound recordings with such information' is a criminal offense, punishable by a fine (100-500 AZN), public works (240-480 hours), or correctional labour (up to one year); and if committed by an official using his official position, then by imprisonment for up to two years (with or without deprivation of the right to hold certain positions or engage in certain activities for up to three years). Moreover, 'unlawful dissemination' in the mass media of recordings (video, voice or photographic) taken 'in the course of proceedings concerning administrative offenses' without the consent of both the person subjected to administrative responsibility and the victim, is punishable with a fine from 1.000 to 1.500 AZN on officials.[252]

In addition to previously established main grounds, the internet content can be taken down if it contains information related to religious 'extremism' or any other religious basis, state secret which can normally be interpreted as being resulted in high treason, espionage, etc. and the most necessary one – defamation. The issue regarding defamation can be solved both under the civil and criminal proceedings. According to Article 23 of the Civil Code ('Protection of honour, dignity and business reputation'), individuals can pursue legal action in courts for information 'discrediting one's honour, dignity or business reputation, violating the secret of one's personal and family life, or personal and family inviolability.' Furthermore, the protection of honour and dignity of individuals is allowed even after the death of the individual. Legal entities can pursue action for information discrediting their business reputation.[253] As to the criminal prosecution of defamatory utterances, options are more abundant. There are four articles in the Criminal Code that provide criminal liability for defamation; Article 147, 148, 148-1, and 323. Article 147 penalises 'slander' which is defined as 'dissemination of deliberately false information discrediting the honour and dignity of another person or undermining his reputation which is done in a public speech, publicly displayed work, in mass media, or publicly disseminated in an internet information resource' Article 148 establishes criminal liability for 'insult', which is defined as 'humiliation of the honour and dignity of another person, expressed indecently in a public speech, a publicly displayed work in mass media, or publicly disseminated in an internet information

252 Article 376 of the Code of Administrative Offenses.
253 Council of Europe, Analysis of Azerbaijani legislation on freedom of expression, 2017.

resource'. The newly added *Article of 148-1* is about the punishing of 'slander or insult committed with using a fake username, profile or account at an internet information resource.' Article 323 is about criminalising 'smearing or humiliation of honour and dignity of the President of the Republic of Azerbaijan in a public speech, publicly displayed work, in mass media, or publicly disseminated on an internet information resource.'

Consequently, freedom of lawful expression of ideas and protection of them is a very crucial matter in Azerbaijan, and the national authoritative bodies use all possible means to develop them in the digital world exclusively.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

Countries, including Azerbaijan, under the European Union, have both a positive obligation to ensure freedom of speech and a negative obligation not to violate the right to freedom of speech of citizens. The basis of freedom of speech and expression in Azerbaijan is granted by the Constitution in Article 47. Relevant to that Article 50 and 51 also constitutionalise freedom of information and freedom of artistic speech respectively. These rights are also applicable to the internet, meaning that citizens have the right to write down their opinions freely. But the content which they are posting on the internet and declaring their thoughts could be taken down based on several reasons. And according to Law of the Republic of Azerbaijan 'On access to information', deleting the internet content is regulated by both the private sector and the government.

By mentioning the private sector, it is usually meant a domain owner or host provider which is defined as 'a legal entity or an individual engaged in entrepreneurial activity that provides telecommunications services using the network of a telecommunications operator.'[254] As it is mentioned in Article 13-2.1. of the law of the Republic of Azerbaijan about and information security, 'the owner of the Internet information resources is independent in determining the content and the rules for placing the information contained in that information resource. The owner of the Internet Information Resource and its domain name must ensure the proper functioning of that information resource and is personally responsible for that.' Deducing from the mentioned article of the law, the issue of blocking and taking down internet content self-regulated by the private sector as well in Azerbaijan.

[254] Law on telecommunication of Azerbaijan Republic Articles 1.0.8 and 1.0.9.

The government also regulates the content of the internet information even if the taking down is self-regulated by the private. For instance, according to the list of the prohibited contents which is mentioned in the law of the Republic of Azerbaijan about information, informatisation, and information security, none of the mentioned content should be posted even if the owner has consented. The regulation of the government about the content of the information has been stricter; consequently, freedom of speech online has been restricted. Internet censorship has been increased through legislative amendments to Azerbaijan's Code of Administrative Offenses in December 2017. To be more precise, according to the Article 388-1 of Azerbaijan's Code of Administrative Offences, fines are imposed on everyone for spreading the context that is prohibited. The list of the prohibited content is mentioned in Article 13 (-20) of the Law of the Republic of Azerbaijan about information, informatisation, and information security.

Before taking down the internet content, the right to be notified is ensured. According to the Law of the Republic of Azerbaijan about information, informatisation and information security, when the relevant executive authority discovers that the information is prohibited from being placed on the internet, or identifying it based on invalid information from individuals, legal entities, or government agencies, it shall notify the owner of the Internet information resource and its domain name and the hosting provider. It is fair enough that the information owner has a right to be notified since another way around deleting the internet content without the owner's consent would be abused by the government.

Grievance redressal mechanism is ensured in terms of complaints, appeals, and inquiry. The inquiry to the information owner is carried out as soon as possible, but no later than seven business days but if this information loses its effectiveness during this time, it should be answered immediately, and if it is not possible, it should be answered no later than 24 hours.[255] If the request is incomplete or inaccurate, the official shall inform the inquirer of the identified deficiencies within five working days.[256] The law also places a commitment onto the owner of the information to help and reply to the inquest, in case they do not do, the inquirer has a right to complain with the Ombudsman. The information owner who executes the request for information explains this right of the applicant and records it in the response (information) provided. Duties by the information-owning state bodies, municipalities and state officials in

255 The Law of the Republic of Azerbaijan on access to information <http://www.e qanun.az/alpidata/framework/data/11/c_f_11142.htm> 14 February 2020.

256 ibid 1.

accordance with the requirements of the Law of the Republic of Azerbaijan On access to information are supervised by the Commissioner, according to the Article 1.3 of the Constitutional Law on Human Rights Commissioner (Ombudsman) of the Republic of Azerbaijan. This provision means that government agencies should respond to appeals or any complaints about deleted online content and the proper function of agencies is controlled by the Commission. Consideration of complaints related to the violation of the right to obtain information is ensured by the Commissioner itself if it fulfils the several requirements mentioned in 13-1.2. Article of the Constitutional Law on Human Rights Commissioner (Ombudsman) of the Republic of Azerbaijan.

After the new legislative amendments to Azerbaijan's Code of Administrative Offenses in December 2017, restricting web pages, blocking internet sites, or taking down internet content by the government has been increased. As a result of amendments, the authorities could block a site if it contains prohibited information having danger to the state or society, and when the website owner cannot remove content within eight hours of receiving notification. Court approval is not required before blocking a website.[257] Authorities firstly restricted some of the websites in March 2017 for containing danger to national security.[258] Against the complaints about these, in December 2017, the Court of Appeal in Baku agreed with the decision of the court in May 2017 that blocked online outlets including Azadliq (Radio Free Europe/Radio Liberty Azerbaijan), Azadliq Daily, Meydan TV, Turan TV, and Azerbaijani Saadi.[259] Later on, in June 2018, the Supreme Court supported the government's decision to block the above-mentioned online media outlets.[260]

To sum up, deleting or taking down the internet content in Azerbaijan is self-regulated by the private sector as well as the government. But in both cases, relevant to the local legislation, several prohibited internet contents have to be taken down.

---

257 Government Blocks Access to Azadliq.info and Azadliq.org Websites in Azerbaijan <https://www.irfs.org/news-feed/government-blocks-access-to-azadliq-info-and-azadliq-org-websites-in-azerbaijan/> 14 February 2020.

258 Eurasianet, Azerbaijan: Government Escalates Hacking Campaign Against Dissent <https://eurasianet.org/azerbaijan-government-escalates-hacking-campaign-against-dissent> accessed 14 February 2020.

259 Open Democracy, Azerbaijan's blocking of websites is a sign of further restrictions online <https://www.opendemocracy.net/en/odr/azerbaijans-blocking-of-websites/> accessed 14 February 2020.

260 Freedom House, Freedom on the Net <https://freedomhouse.org/report/freedom-net/2018/azerbaijan> accessed 14 February 2020.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

When individuals perform some wrong acts in the past, they are not necessarily held accountable for their past actions and their fault should not be perpetual. Therefore, people have a right to be forgotten, meaning that negative personal information about them could be removed from the internet resources by their request or if the data does not serve its original processing aim. This issue has been discussed in the European Union based on the point that individuals have a right to change their life and live autonomously after their wrong acts. Based on these justifications, Azerbaijani legislation also ensures the right to be forgotten within the right to delete the personal data which relates the information either directly, or indirectly to whom personal data relates.

İssues related to the personal data in Azerbaijan are mostly regulated by local legislation, for instance, Law of the Republic of Azerbaijan On Personal Data ('Law') as well as other legislative acts related to data privacy. According to the mentioned law, people have a right to request their information to be deleted. To be more precise, Article 2.1.17 of the above-mentioned law of Azerbaijan states that the deletion of personal data shall mean the deletion of personal data from the operating system. But it needs to be more concrete because in the law this right is ensured by generally mentioning deleting personal data. However, personal data could be deleted in several ways; upon the person's discretion, deleting by the hosting provider or after the date of the personal data expired. Thus, the right to be forgotten needs to be mentioned separately in the legislation since it refers only to delete the personal data upon the information owner's request.

According to the Azerbaijani Law on Personal Data, processing of a personal data about any individual shall be permitted only with the written consent of the individual and the following information must be included in the subject's consent:

- information allowing the identification of the data subject;
- information allowing the identification of the owner or operator which has obtained the consent of the data subject;
- the purpose of collection and processing of personal data;
- a list of personal data in respect of which the data subject has provided its consent including the list of processing operations for such data;
- the period during which the consent remains valid and the circumstances in which consent can be revoked; and

— the terms for the deletion and archiving of personal data in the event of data subject's death and/or expiration of the storage term for personal data.

When the data subjects receive the information from the 3rd parties or transmit it, then the subject's consent is again required.[261]

Azerbaijan follows similar proceedings for the right to be forgotten as in the EU. For example, the identification of the data subject must be proven. If not proven, the data could be not deleted from internet resources. But it is not the case for the data prohibited with statutory, since erasure must be quick, not later than the due date.

Additionally, the Right to be Forgotten requires notification obligation as it is in the European Union. As it is mentioned in Article 19 of the GDPR 'The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out under Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.'[262] Deducing from this provision, the data subject also has a right to be notified about the erasure of the data. It also ensures if the data subject himself/herself wants the information to be deleted or not.

6. How does your country regulate the liability of internet intermediaries?

Regulations by the European Union encompasses Azerbaijan as well. Several aspects of information society services, including freedom of services, the treatment of electronic contracts, and liability issues for third party content is regulated.[263]

The liability of the internet intermediaries in Azerbaijan is also regulated based on the local legislation and obligation to implement the measures for blocking

261 Cis-legislation: Law of the Azerbaijan Republic about Personal Data <https://cis-legislation.com/document.fwx?rgn=31412> accessed 14 February 2020.

262 The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

263 European Union and Google Spain <https://publixphere.net/i/noc/page/OI_Case_Study_European_Union_and_Google_Spain> accessed 14 February 2020.

and taking down content exist. They are subject to statutory erasure obligations. To give an example, according to the law of Azerbaijan on information, informatisation and information security, if information that is prohibited for dissemination is found on the website, the relevant executive body will warn the owner of the content and its host provider. The site owner has to delete the content when receiving a notice immediately. If the information is not taken down within eight hours after the notification, restriction to the website could be demanded. If this information threatens the state and public, the site will be shut down without a court order and then will apply to the courts.

In general, internet intermediaries must not allow the following information:

- 'propaganda and financing of terrorism, as well as methods and means of terrorism, information about training for the purpose of terrorism, as well as open calls for terrorism';
- 'information on the propaganda of violence and religious extremism, open calls directed to the evocation of national, racial or religious enmity, violent change of the constitutional order, territorial disintegration, violent seizure or maintenance of power, organization of mass riots';
- state secrets;
- 'instructions or methods for producing firearms, their parts, ammunition, and explosive substances'
- 'information on preparation and usage of narcotic drugs, psychotropic substances, and their precursors, about locations of their unlawful acquisition, as well as information on the location of and methods of cultivation of plants containing narcotic substances';
- 'pornography, including information related to child pornography';
- 'Information on the organisation of and incitement to gambling and other unlawful betting games';
- 'information disseminated with a purpose to promote suicide as a method of solving problems justifies suicide, provides a basis for or incites to suicide, describes the methods of committing suicide, and organizes commission of suicide by several individuals or organized group';
- 'defamatory and insulting information, as well as information breaching inviolability of private life';
- 'information breaching intellectual property rights';

— other information prohibited by the laws of the Republic of Azerbaijan.[264]

If such information is posted, erasure of that information from the resource must be ensured.

Having the authority to take down the content should not be the channel to the restriction of freedom of speech and abuse by the internet intermediaries. According to the Council of Europe standards with regard to freedom of expression on the internet, 'any measure was taken by State authorities or private-sector actors to block, filter or remove Internet content or any request by State authorities to carry out such actions must comply with the requirements set by Article 10 of the Convention. They must, in particular, be prescribed by a law that is accessible, clear, unambiguous, and sufficiently precise to enable individuals to regulate their conduct. They must at the same time be necessary for a democratic society and proportionate to the legitimate aim pursued.'[265]

However, there are exceptional cases when the liability of the internet intermediary exists. In the E-Commerce Directive, types of illegal content and activities (infringements on copyright, defamation, content harmful to minors, unfair commercial practices, etc.) and different kinds of liability (criminal, civil, direct, indirect are exempted.[266] Even if the internet intermediary is not exempted, they could not necessarily be liable. The intermediary may have no more immunity provided by the E-Commerce Directive. Liability is then being questioned respectively to the specific law in each Member State.[267]

---

264 Article 13-2.3 of the Law on the telecommunication.

265 Partnership for good governance: Analysis of Azerbaijani legislation on freedom of expression <https://rm.coe.int/azerbaijan-analysis-of-legislation-on-freedom-of-expression-december-2/16808ae03d> accessed 14 February 2020.

266 European Parliament Directorate-General for Internal Policies, Providers liability: From the eCommerce to directive future <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf>.

267 Legal analysis of a Single Market for the Information Society Chapter 6: Liability of Online Intermediaries November 2009, page 10 <http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=842> accessed 14 February 2020.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

The Republic of Azerbaijan is still on the level of development of the internet system, and relevant legislation regarding online content blocking and takedown, the circumstances allowing the right to be forgotten and the liability of internet intermediaries. Although, bringing the internet intermediaries into liability is not something that should be fully regulated under the national law. National law such as the appropriate legislation of Azerbaijan on this issue can only put some directives to take intermediaries to liability in conformity with the own guidelines of each Internet Service Providers (ISP's) and Internet Content Providers. The right to be forgotten, on the other hand, has been explicitly defined under the informational laws and pertinent articles of the National Codes of the Republic of Azerbaijan. Nowadays, online content blocking or takedown is a controversial issue, because of a number of changes have been made to this field recently.

In fact, Azerbaijan before its independence was a part of the USSR, the country where the violations of freedom of expression were huge of its time. Therefore, shifting immediately from a colonised country where any rights were restricted to the democratic and law-governed republic has left its negative effects for years. Moreover, one may claim that then why Estonia, another post-soviet country that can be considered as in the same situation with Azerbaijan after the dissolution of the USSR, now became a digital country. The answer to this question is hidden behind the number of population factors of each country. The current population of Estonia is 1.326.148 as of Thursday, 23 January 2020, based on a Worldometer elaboration of the latest United Nations data which is smaller than Azerbaijan's. Henceforth, the establishment and construction of the sustainable digital world and maintaining it alongside with promotion of affordability and high-speed internet system is much easier with a smaller population living in approximately the same coverage of the territory.

The development programme of Azerbaijan with the Council of Europe is called 'Council of Europe Action Plan for Azerbaijan 2018-2021.' Based on this programme, it can be said, that Azerbaijan within less time will accomplish its aim of providing a better quality of the informational and technological system for the community. Furthermore, the encouragement and motivational effects of it for the next years are even foreseeable in advance. Additionally, while talking about state programs, 'The State Program on the development of communication and information technologies in Azerbaijan' has also a great

place on the informational improvement history of Azerbaijan as the first step in-country for implementation of the plan of 'Electron Azerbaijan'. Nowadays, the most influential program is assumed to be the 'The government's Strategic Roadmap programme' that seeks to better information and communication technologies by providing internet speeds of 20 Mbit/s by 2020 and 50 Mbit/s by 2025.[268] The actions are taken in any spheres of informational law, even the speed of internet are linkable, therefore increasing the speed will have positive impacts on growth in freedom of expression, freedom of information, actions taken by relevant government bodies to control and promote internet, and ultimately on the establishment of 'Digital' or 'Electron' Azerbaijan.

According to the report of Freedom House of 2018 on Azerbaijan, these days the Ministry of Transport, Communication, and High Technologies (MTCHT) holds significant shares in a handful of leading internet service providers (ISPs), and the government is authorised to instruct companies to cut internet service under very broadly defined circumstances, including war, emergencies, and national disasters, 'In previous years, the government refrained from extensive blocking or filtering of online content, relying on legal, economic, and social pressures to discourage critical media coverage or political activism. Authorities initially restricted some of the websites in March 2017 for threatening national security and containing content that promotes 'violence, hatred, or extremism' and 'violated privacy, or constituted slander.'[269]

The 2018 report of Freedom House briefly explains the procedure of the removal of internet content under Azerbaijani legislation: 'Based on this, on 10 March, changes and amendments were made to Information, Informatisation and Protection of Information and on Telecommunications by Milli Mejlis (Parliament). According to the amendment, during the detection of unlawful information on a website, the relevant executive authority (expected to be the Ministry of Transport, Communications, and High Technologies) will immediately warn the website and its host provider. Upon receipt of the warning, the website owner is obliged to immediately remove that information from the website. Unless the prohibited information is deleted within eight hours of warning, the relevant executive authority shall appeal to the court to restrict the website. If the information poses a danger for the state or society, the relevant authority will shut down the website without a court decision and then apply it to the court. Access to the website restricted by the authority will be blocked until the completion of judicial review. The court will consider this appeal within

268 Report of Freedom House on Freedom on the Net 2018 in Azerbaijan <https://freedomhouse.org/report/freedom-net/2018/azerbaijan> accessed 20 February 2020.

269 ibid.

five days.'[270] According to the new law, the owner of an internet information resource and its domain name should avoid uploading the following prohibited information on that information resource:

- information on promotion and financing of terrorism, methods and tools of carrying out terrorist acts, and organising or conducting training with the purpose of terrorism, as well as open encouragement of terrorism;
- information on promotion of violence and religious extremism, and open encouragement of national, racial or religious hatred and enmity, violent change of the constitutional system of the state, the disintegration of territorial integrity, violent seizure and retention of power, and organisation of mass disorder;
- information constituting a state secret;
- information on procedure and methods of preparing firearms, component parts, ammunition, or explosives;
- information on methods and procedure of preparation and use of narcotic drugs, psychotropic substances and their precursors, places where they can be illegally purchased, as well as places and methods of cultivation of plants containing narcotic drugs;
- information on pornography, including child pornography;
- information encouraging organisation of gambling and other illegal betting games and participation in such games;
- information promoting suicide as a solution to problems, condoning suicide, justifying or encouraging its committal, explaining methods of committing suicide, or information disseminated with the purpose of organising a group suicide of several people;
- information of an offensive and libellous nature, as well as information violating privacy;
- information infringing intellectual property rights;
- Other information prohibited from dissemination by laws of Azerbaijan.

From this point of view, it can be derived that recent legislative amendments enable the government to block or takedown any website posing a danger to the state or society. Based on the order of the Ministry of Transport, Communications and High Technology, this preventive blocking mean requires

[270] Government blocks access to azadliq.info and azadliq.org websites in Azerbaijan, 27 March 2017 < https://www.irfs.org/news-feed/government-blocks-access-to-azadliq-info-and-azadliq-org-websites-in-azerbaijan/> accessed 20 February 2020

subsequent approval by a court.[271] It is defined in the 2018 report of Freedom House as 'A formality in a country where the justice system acts as the executive's armed wing.'[272]

Another step on the improvement of the internet system was made at a National Parliament Human Rights Committee meeting in January 2017, Chairman of the Press Council Aflatun Amashov discussed creating legislation to monitor and regulate bloggers and social media platforms.[273]

The next actions in the sphere of reinforcement of the internet system in all areas in Azerbaijan were made and have still been made in the field of adoption of new articles of Criminal, Administrative or Civil law and even making amendments to them. The first indications were firstly observed during November 2017 and those, relevantly have inevitable supremacy over the development of the rules on blocking and takedown of internet content, right to be forgotten, liability for intermediaries and other issues regarding this common approach. In November 2016, penalties were increased for online insult and libel which entail blocking of the internet content and even maybe resulted in liabilities for intermediaries. A new provision to Article 148(1) of the Criminal Code targeted insult or slander disseminated online by fake usernames or accounts. The increased penalties include a fine of AZN 1.000-1.500 (about US$590-885), community service for 360-480 hours, or corrective labour for up to one year.[274] Moreover, the most important decision was the adoption of new articles such as Article 147(1) of the Criminal Code which targets the 'dissemination, in a public statement, publicly exhibited work of art, through the mass media or a publicly displayed Internet information resource, of knowingly false information discrediting the honour and dignity of a person or damaging his or her reputation.'[275] The new penalties imposed include a fine of AZN 1.000-1.500, community service for 240-480 hours, corrective labour for up to one year, or imprisonment for up to six months. According to Article 147(2), libel becomes punishable by corrective labour for a term of up to two years, or

---

271 RSF, Online censorship rounds off Aliyev's control of Azerbaijani media. 3 May 2017, <https://rsf.org/en/news/online-censorship-rounds-aliyevs-control-azerbaijani-media> accessed 20 February 2020.

272 Report of Freedom House on Freedom on the Net 2018 in Azerbaijan <https://freedomhouse.org/report/freedom-net/2018/azerbaijan> accessed 20 February 2020.

273 Report of Freedom House on Freedom on the Net 2018 in Azerbaijan <https://freedomhouse.org/report/freedom-net/2018/azerbaijan> accessed 20 February 2020.

274 2016 Country Reports on Human Rights Practices – Azerbaijan, U.S Department of State, 3 March 2017 <https://www.state.gov/j/drl/rls/hrrpt/2016/eur/265396.html> accessed 20 February 2020.

275 OSCE the Representatives of Freedom of the Media Dunja Mijatovic, Defamation and insult laws in the OSCE region: A comparative study, March 2017 <https://www.osce.org/fom/303181?download=true> accessed 20 February 2020.

by imprisonment for a term of up to three years when it accuses someone 'of having committed a serious or especially serious crime.'[276]

Currently, the people of Azerbaijan have the exclusive right to be forgotten most importantly, under 'The Law on Mass Media' of 1999 the information about which has been given in previous research questions. The steps were taken by the Azerbaijani government especially right after 2016 play a great role in defining the informational situation of Azerbaijan over five years and taking down the obstacles on the promotion of it in the future. The Republic of Azerbaijan, at this moment, is on the verge of transmission to the digital and electronic world through these.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

As far as it is concerned, freedom of expression in any form creates some responsibilities and liabilities on its own. It requires reasonable effort and effective mechanisms to prevent the necessary balance between to provide one's rights and freedom and to protect the interest of other members of society or society as a whole. As in the legislations of various countries, this issue has been addressed in also Azerbaijani legislation, by diverse legal normative legal acts.

One problem that could be potentially caused by abuse of freedom of expression online, is the usage of this right to make hate speeches against the reputation and personality of others. This issue is much more widespread in the virtual environment since the internet promotes the opportunity to spread one's opinions without much interference or public censure. It is also more satisfactory from the point of being more broadly available to the audience, thus harmful on a wider scale. Considering these points, this problem has been dealt with in various aspects of law, accompanied by diverse legal normative acts.

First of all, it is essential to note that as Azerbaijani legislation holds a monist approach to international law, the international conventions are an inseparable part of the legislation in this sphere. That approach is stressed in the second part of Article 148. In the other fields, the legal force of the conventions is below the constitution, as noted in the Article 151 that in case any contradictions exist

[276] The criminal code of the republic of Azerbaijan, <http://www.e-qanun.az/code/11> accessed 20 February 2020.

between the legal normative acts of the Republic of Azerbaijan (except for the Constitution and the acts adopted via referendum) and the international treaties that it has entered, the treaties are forced. Here it is clear that although the international treaties have higher legal force than the legislation, the Constitution is above this hierarchy. However, the second part of Article 12 states that the fundamental rights mentioned in this Constitution must be applied in accordance with the international treaties. This article implies the superiority of international human rights.

The primary source of legislation of the Republic of Azerbaijan on human rights is considered to be the European Convention on Human Rights (ECHR). Article 10 of the ECHR secures everyone the right to freedom of expression, also defines the scope and limit of this right. This provision includes also the right to receive and impart information without interference by public authority. Nevertheless, in order to reach the balance between protecting this right and other rights, the second part of the article reminds the responsibilities and duties that accompany the implementation of this right and defines some cases where it could be necessary to levy restrictions and penalties for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others. Taking into account the menace that the hate speeches are creating for people, based on the fact that it is usually targeted at people because of their sex, race, ethnicity, etc, we can conclude that it is covered in this article.

Secondly, another important source of the legislation of the Republic of Azerbaijan, the Constitution deals with the protection and regulation of the freedom of expression as well. As mentioned above, in accordance with the ECHR, the Constitution of the Republic of Azerbaijan secures everyone the freedom of speech in Article 47. Also, the third part of the same article directly forbids the propaganda and agitation which incites hatred and hostility based on race, nationality, religion, social status or any other criteria. Apart from that, freedom of expression and sources of public information are guaranteed. The second part of Article 50 prohibits the state censorship in the sources of information, also media.

Various degrees of the potential problems caused by abuse of the right to freedom of expression are addressed in different areas of law such as administrative, civil, criminal law etc. In these areas, the relevant normative legal acts are the codes adopted by the parliament. In this sense, the importance of the criminal code is more significant, as it deals with more extreme forms of violence and it directly applies to insult and hate speeches online.

Above all, two types of such violations are differentiated in the Criminal Code of Azerbaijan according to the method it is committed. Article 148 of the Criminal Code defines the situation to which this provision can apply and the appropriate penalty for insulting someone. It includes also to degrade one's honour and dignity on the Internet. The penalty applied for this provision includes several alternatives, such as a fine of 1000-1500 manat, 240-480 hours public work or reformatory activities up to one year or imprisonment for up to six months.

However, the additional provision in the Criminal Code addresses a very particular situation in which this violation takes place via fake profiles and accounts. Article 148-1 sets higher penalties than the ones set for the provision of Article 148. Here, the penalty of fine is 1000-2000 manat, the public works 360-480 hours, reformatory activities up to 2 years and imprisonment up to 1 year. Appointment of additional provision for this purpose may be linked to the better situation of those who hide under the fake usernames so that they do not incur any public blame.

In addition, the legislation protects the honour and dignity of the President via special provisions. Article 323 defines different punishments if this violation is targeted at the President, which is reformatory activities or imprisonment both up to two years. According to the 323.1-1, if this offense is done via fake usernames or profiles, the punishment is imprisonment for up to three years.

Nonetheless, despite all the normative legal acts and the legislation that provides for freedom of expression online, protection of this right in practice is being challenged. According to various cases against Azerbaijan and reports, the main causes of this are political reasons. One of the cases brought before the European Court of Human Rights, *Khadija Ismayilova v. Azerbaijan*, is a good example of the violations of this right.

The applicant, Khadija Isamyil is a well-known journalist in Azerbaijan and has incurred harassment such as the invasion of her private life and threat of public humiliation by dissemination of her intimate video. The court assessed the allegations and determined that there had been violations of Article 8 (right to respect for private and family life) and Article 10 (freedom of expression). The court also determined that 'the acts of a criminal nature committed against the applicant were linked to her journalistic activity; no other plausible motive for the harassment she had to face has been advanced or can be discerned from the case file.'[277]

[277] Khadija Ismayilova v. Azerbaijan [2019] ECtHR.

Another serious fact proving these kinds of allegations in the reports that were presented before the court about the general situation in Azerbaijan from the point of protection of the right of expression. Report by the Commissioner for Human Rights of the Council of Europe (CommDH(2013)14, dated 6 August 2013) described the practice of freedom of expression in Azerbaijan. According to this report, journalists experienced intimidation, violence, and judicial harassment because of their activities, 'According to the prison census conducted by the Committee to Protect Journalists (CPJ) in December 2012, Azerbaijan ranked among the top countries jailing journalists with nine imprisoned journalists.'[278]

To sum up, the answer to the question of whether the balance between the freedom of expression online and the prevention of hate speeches online, it should be noted that the practice of this freedom is not as satisfactory as required despite the legal mechanisms to provide it.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

The practice of the right to freedom of expression requires a satisfactory balance in accordance with the practice of other rights apart from the prevention of hate speeches online. This essay is targeted to define those rights and the challenges which are standing in front of reaching such balance, also analyse the relevant legislation on this issue.

It also has to be noted that as the appropriate provisions for the freedom of expression have been mentioned in the previous question, more attention will be paid to demonstrate the provisions for other rights which we will analyse in connection with freedom of expression.

First of all, starting from the top of the hierarchy of the legal acts on this topics, Article 10.2, the provision of the European Convention of Human Rights which mentions the responsibilities and duties that will be necessary to control in a democratic society for goals such as the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[278] ibid.

Article 32 of the Constitution of the Republic of Azerbaijan secures everyone the right to personal immunity. This provision includes the right to personal and family rights and states the unacceptability of the interference with that right except for some cases mentioned there. Any form of interference is addressed, including disseminating one's personal information, gaining data, videos, photos, etc and spreading it without their approval. Violation of this right creates legal liabilities in civil, administrative or criminal norms.

Protection of one's professional reputation is provided within the civil law, more precisely, Article 23. This protection applies not only to the physical also to the legal persons. Article 23.4 allows the one whose rights have been violated to demand them to compensate for damages caused. The provision also targets to protect one's honour and dignity in addition to the professional reputation.

Protection of professional reputation can also be endangered when there is a case of slander, which means spreading information about someone o the public information sources while knowing that it does not reflect the truth. The criminal penalty has been established for this violation under Article 147 of the Criminal Code. However, the penalty is different in attitude with the scope of the slander. While the penalty for slander has been determined as monetary fine of 1.000-1.500 manats, public work of 240-480 hours, reformatory activities up to one year or imprisonment up to six months, in case the disseminated information is about grave or especially grave crimes, the penalty becomes reformatory activities up to two years or imprisonment up to three years.

The tort law of the Republic of Azerbaijan, which is included in the administrative law, and regulated via the Code of Administrative Offences, also establishes some rules and penalties for breach of these rules related to the freedom of expression online, including media. Article 388-1 of the Code defines punishments for disseminating information that has been forbidden by the relevant legislation.

In order to protect the children from harmful information, the Code of Administrative Offences appoints some obligations for disseminating a definite category of data. Article 388-2 includes the requirements such as marking the age requirement, restricting the spread of information among children by providing a warning when a piece of information that is not appropriate for kids is spread. The violations of this provision cause any person to pay a monetary fine of which amount is determined depending on the offender. If the offender is a physical person, the fine is 500-1000, legal person 1.500-2.500 and in case it is an official, the amount is 3.000-4.000 manat.

The law about media is one of the primary sources of legislation in regulation of the freedoms and restrictions on media. Article 10 of this normative legal act deals with cases of abuse of the freedom of media. It includes propaganda that incites war and intolerance based on race, nationality, to spread secret information that is protected by legislation, publishing misleading information that damages honour and dignity of people under a name of a valid source and dissemination of pornographic materials.

Prohibition of pornography is common in the legislations of numerous countries. The main basis for that is the protection of public morals, which has been stated also in Article 10.2 of the European Convention on Human Rights.

However, the development of an online environment brings some challenges as well as advantages. In some countries it enables the authorities and individuals to abuse the advantages of the internet and utilise it to violate human rights. Due to the accessibility to everyone, ability to reach to a greater audience and the opportunity to hide one's identity, most violations like slander, hate speeches, insulting, degrading human honour and dignity, damaging one's professional reputation, spreading private information, etc, happen on a greater scale on the internet. All the legislation mentioned above has been adopted to prevent such cases.

In conclusion, reaching an adequate balance between the freedom of expression online and protecting other rights, is a purpose that needs to take time and undergo a long process for being achieved. Although the normative legal acts and the international treaties are not enough on their own, they are a step towards the future elimination of this type of violations.

10. How do you rank the access to freedom of expression online in your country?

Over the past few years, the development of technology and increased consumer demand has made it possible for more people to access the Internet, which has led to an increase in the number of Internet users both in Azerbaijan and around the world.[279] Currently, a third of the Azerbaijani population has access to the Internet, which has turned the internet into a platform for information sharing.

[279] Report of Freedom House on Freedom on the Net 2011 in Azerbaijan < https://www.freedomhouse.org/sites/default/files/inline_images/Azerbaijan_FOTN 2011 .pdf> accessed 20 February 2020.

In parallel with the rise in internet usage, there has also been an increase in the number of people having access to the internet and limiting their online activity.

The internet in Azerbaijan may be considered partly free. However, after the Internet Governance Forum held in Baku in 2012, especially in the first quarter of 2013, there were many concerns in this area.[280]

The biggest threat to online freedom of expression has been government crackdown on individuals who have made critical comments on the Internet. Although technically Azerbaijanis can do what they want on the internet, there can be no guarantee that this will not lead to undesirable results. On the contrary, if someone passes a certain threshold when commenting on the Internet, for example, calling for a protest, revealing facts of corruption, he puts himself in grave danger.

The persons who use Facebook to protest are subject to a high fine in line with recent changes to the Freedom of Assembly Act. For example, on January 26 2020, activist Turgut Gambar was fined 2.500 manat for calling on Facebook to protest. Emin Milli, who was previously arrested on the same charge, received a fifteen-day administrative sentence. The court's decision stated that young activists had called on citizens to take part in an illegal protest by posting illegal calls on Facebook.[281]

Although the Azerbaijani authorities are increasingly trying to control the internet, the internet may be considered less restrictive than most print and broadcast media, the main source of news for most citizens. The media law, adopted in 1999, considers the Internet a media outlet. For this reason, all the problematic rules of law that apply to the media can be applied to regulate the Internet. The Ministry of Communications and Information Technologies (MCIT) is the main body responsible for regulating the Internet in the country.[282] However, experts stress the importance of delegating this function to another body outside the state's control. The Ministry also imposes restrictions on the national domain name 'AZ'.

---

280 Institute for Reporters' Freedom and Safety, 2013 First Quarterly Freedom of Expression Report <https://www.irfs.org/wp-content/uploads/2013/05/IRFS_Q1_2013-Azerbaijan-report.pdf> accessed 29 July 2020.

281 Facebakers, Facebook Statistics Azerbaijan <http://www.facebakers.com/countries-with-facebook/AZ/> accessed 1 January 2011.

282 Law of the Republic of Azerbaijan About Mass Media, Azerbaijan National Academy of Sciences <http://ict.az/en/index.php?option=com_content&task=view&id=477&Itemid=95> accessed 29 July 2020.

While online media is free from censorship in Azerbaijan, the authorities have also sought to control this media.[283] From government officials' statements, it is clear that legal mechanisms to control the Internet (such as online television licenses) may soon be applied. For example, in a statement issued on January 10, the head of the National Television and Radio Council, Nushiravan Maharamli, said online television should be licensed, as is the case with traditional television channels.

IRFS is also deeply concerned about plans to pass a law that will give the government the right to regulate the Internet widely, with the purpose of 'protecting children from pornography and other harmful content on the Internet.'[284] Because, under authoritarian regimes, the passage of such a law often results in technical censorship of the internet. For example, government agencies are developing a blacklist of prohibited sites and access to these sites is blocked.

11. How do you overall assess the legal situation in your country regarding internet censorship?

The freedom of expression online and in any other form is protected via the legislation which includes not only the local normative legal acts, also the international treaties it is subject to. As freedom of expression is considered one of the fundamental human rights, the local regulatory mechanisms on this issue, including the Constitution, must be in accordance with the international treaties that Azerbaijan has entered.[285] This statement is reflected in Article 12 of the Constitution.

Therefore, above all the legislation on freedom of expression, comes the European Convention on Human Rights, since Azerbaijan ratified the convention in 2002. Article 10 of the European Convention on Human Rights guarantees everyone freedom of expression, which includes freedom to hold opinions without interference by public authorities and regardless of frontiers.

Starting from the local legislation, the Constitution of Azerbaijan also contains the provisions for the protection of this right. Article 47 emphasises the freedom of thought and expression and states that 'No one shall be compelled to express his views or beliefs or to renounce his ideas and beliefs.' Article 50 states that

283 Report of Freedom House on Freedom on the Net 2011 in Azerbaijan <https://www.freedomhouse.org/sites/default/files/inline_images/Azerbaijan_FOTN2011.pdf> accessed 20 February 2020.

284 Law of the Republic of Azerbaijan About Mass Media, Azerbaijan National Academy of Sciences <http://ict.az/en/index.php?option=com_content&task=view&id=477&Itemid=95>.

285 Article 12 of the Constitution of Azerbaijan.

"Everyone has the right to seek, receive, transmit, prepare and impart information that everyone wants." State censorship on mass media, including the press is prohibited and freedom of mass media is guaranteed.[286]

However, there is no unlimited freedoms and as Article 71 of the Constitution states that the rights and freedoms secured by this Constitution can only be restricted on the grounds defined by this Constitution and other legislative acts, and also via the rights of other people. In addition, Article 10 of ECHR also defines some cases where such restrictions can be essential in a democratic society. There are different methods of restriction of freedom of expression online.

As mentioned in the previous questions, along with the international treaties and the Constitution of Azerbaijan, there are also laws adopted by Milli Majlis (Parliament) that regulate the blocking and takedown of the internet content. One of the most important laws on this issue may be 'Law on Mass Media' which was adopted in 1999. Another example can be the 'Law of the Republic of Azerbaijan on telecommunications.' Regulations on the issue of informational law, as well as the cases when the internet content may be blocked or taken down, are submitted in the 'Law of the Republic of Azerbaijan on accession to the Charter and the Convention on the International Telecommunication Union as well as the adjustment documents.'

The regulations on this issue are also reflected in civil, criminal and administrative codes of Azerbaijan in different levels and forms. The grounds for that kind of action have been shown in the relevant codes. It includes defamation through the internet, arising national, religious, or any other conflicts within the usage of internet, dissemination of children pornography and other actions constituting threats against state security and integrity.[287]

In Azerbaijani legislation, the government plays a significant role in blocking and taking down the content, even if this act is implemented by the private sector. The list of the prohibited contents which is mentioned in the 'law of Republic of Azerbaijan about information security' does not let any of the mentioned content should be posted even in the case the owner has consent.

In addition, the law mentioned above ensures the right to be notified[288], without which the freedom of expression online would be threatened by the government

286 Article 50 of the Constitution of Azerbaijan.
287 Article 10 of the Law on Mass Media of the Republic of Azerbaijan.
288 Article 13-3 of the Law of Republic of Azerbaijan about information, informatisation and information security.

in a significant deal. It requires notifying the owner of the resource and its domain name and the hosting provider.

In the overall assessment, the regulation between the freedom of expression and the right to be forgotten cannot be ignored. The Law of the Republic of Azerbaijan On Personal Data defines some rules of deleting one's personal information from the operating system.[289] The ways that can happen include upon the person's discretion, deleting by the hosting provider, or after the date of the personal data expired.[290] Also, in such cases, the identification of the data subject must be proven.[291] If not proven, the data could not be deleted from internet resources.

Abuse of the freedom of expression can danger another fundamental human right such as the right to private and family life. Thus, a number of provisions are targeted to reach an adequate balance between these rights. Article 32 of the Constitution confirms the right to personal immunity including the right to private and family life and also ensures protection from the cases such as dissemination of one's personal information without their consent, attempt to gain information about them from the sources of information online or in any other forms except for situations regulated by law.

Certain provisions in the Civil Code of Azerbaijan attempt to protect individuals from this type of violations by defining the liabilities of the offender. Article 23.4 allows the one whose rights have been violated to demand them to compensate for damages caused because of the offense against their professional reputation.

This right is also protected via the Criminal Code, of which Article 147 prohibits slander, and Article 148 defines penalties for the crime of insult. These provisions are aimed at protecting both professional reputations, and human honour and dignity as well. The Code of Administrative Offences also establishes some rules and penalties for breach of these rules related to the freedom of expression online, including media. Article 388-1 of the Code defines punishments for disseminating information that has been forbidden by the relevant legislation.

The subjects of the liabilities and penalties can also be the internet intermediaries, although in exceptional cases. In the E-Commerce Directive, types of illegal content and activities and different kinds of liability are

289 Article 2.1.17 of the Law of the Republic of Azerbaijan On Personal Data.
290 Article 8 the Law of the Republic of Azerbaijan On Personal Data.
291 Article 8.2.1 the Law of the Republic of Azerbaijan On Personal Data.

exempted.[292] Even if the internet intermediary is not exempted, they could not necessarily be liable. The intermediary may have no more immunity provided by the E-Commerce Directive.

Overall, evaluating the current situation about the provision of the freedom of expression in Azerbaijan, still adequate balance does not seem to have been achieved despite all the provisions and the legislative acts on this issue.

First of all, the freedom of mass media and the internet is violated by the government in some cases. As mentioned in the previous questions, this statement is supported by cases brought before the European Court of Human Rights and international reports. The case of Khadija Ismayilova vs. Azerbaijan was a clear example of this topic.

The violations are more common against the journalists, nonetheless, some were targeted just because of an opinion or critical comments shared on the social media. The usage of the internet, which is thereby considered partly free, by the government to target the individuals critical of the government creates great concerns in this sense. The example of Turkel Alisoy, who was a member of the PFPA Youth, is appropriate for this concern as well. He was held liable to criminal punishment for calling 'illegal' protests on Facebook.[293]

However, as it was discussed above, taking into consideration of the Soviet past of Azerbaijan, where the human rights violations were taking place in wide scales, and the fact that democratic traditions are just starting to develop, one can have reasonable grounds to hope for better protection of human rights, including the freedom of expression in the next five years. Also, another challenge is the fast developments in the area of the internet and digital market, therefore the laws and regulations are still not quite stable since this process is still going on. Besides, Azerbaijan has taken steps towards the improvement of this situation by joining the international conventions and programs. 'Council of Europe Action Plan for Azerbaijan 2018-2021' is one of the examples in order to provide a better quality informational and technological system.

[292] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[293] Today.az, Control Over Online Sources and Facebook-like sites in Azerbaijan, 27 November 2010 <http://www.today.az/view.php?id=77287> accessed 29 July 2020.

Conclusion

Censorship on the Internet concerns one of the fundamental human rights, freedom of expression, which has been accepted so by the numerous conventions dealing with human and citizen rights and freedoms, including the European Convention on Human Rights, International Covenant on Civil and Political Rights, Universal Declaration of Human Rights etc.

However, as it was mentioned above, there is not unlimited freedom, and in some cases, restrictions on some rights can be inevitable since it can collide with the rights of others.[294] In those kinds of cases, special attention must be paid to whether these restrictions are proportional to the aim to be achieved because the limitations also cannot be exercised unlimitedly.[295] In order to avoid giving the governments a wide margin of appreciation in this area, the Article 10.2 of the European Convention on Human Rights precisely deals with this matter and determines the conditions on which such restrictions can be levied.

Despite the legal mechanisms for protecting the freedom of expression online, it is a fact that some breaches occur in practice. These violations happen as a result of the abuse of authority to suppress people with different political opinions. Cases of people prosecuted because of their expression online, for instance, by sharing information or revealing one's opinion have been recorded which form a valid proof of the existence of the violations of freedom of expression online. This statement has been claimed above and supported by some evidence of cases of Turgut Gambar, Emin Milli,[296] and Turkel Alisoy.[297]

However, in comparison with other sources of information, the internet is the least controlled and offering more freedom from the point of freedom of expression. Statistically, today the internet is being used by approximately three billion people[298] and steps are being taken to enable more people to have access to the Internet. With such a number of users and popularity, the Internet, among the other sources of information, serves most to the exchange of information and ideas. So, in order to provide pluralism and tolerance, which are necessary for a democratic society,[299] the Internet plays a significant role and restricting the

294 Article 71 of the Constitution of the Republic of Azerbaijan (1999).
295 Article 18 of the European Convention on Human Rights.
296 Facebakers, Facebook Statistics Azerbaijan <http://www.facebakers.com/countries-with-facebook/AZ/> accessed 1 January 2020.
297 Today.az, Control Over Online Sources and Facebook-like sites in Azerbaijan, 27 November 2010 <http://www.today.az/view.php?id=77287> accessed 29 July 2020.
298 International Telecommunications Union, The World in 2014: ICT Facts and Figures.
299 European Court of Human Rights Internet: case law of the European Court of Human Rights, June 2015 <https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf> accessed 29 July 2020.

freedom of expression online creates great concerns for the further development of democracy.

In conclusion, although certain breaches of the freedom of expression online happen, it can be argued that these cases can perish as democracy will be deeply rooted. As mentioned above, Azerbaijan like some other countries has undergone a long period of dictatorship regimes, where such violations were common. In this case, this process will require of time and effort by the people.

Table of legislation

Provision in Azerbaijani language	**Corresponding translation in English**
İnsan Hüquqları Bəyannaməsinin 19cu maddəsinin A bəndinin 3cü hissəsi 217 1948	GA Res 217 A(III) art 19 [UNDR] Universal Declaration of Human rights 1948 (Freedom of belief)
İnsan hüquqları bəyannaməsinin 20ci maddəsi 1948(Dinc yıgıncaqlar və assosasiyalar azadlığı)	Article 20. Universal Dec.of Human rights 1948(freedom of peaceful assembly and associations)
Mülki və Siyasi hüquqlar haqqında paktın 171ci bəndi 21ci fəsil 1966	Res(2200A(XXI)999 UNTS 171 International Covenant on civil and political rights 1966
Avropa Konvensiyasınin 10(1), 10(2) ci mad. 1950(İşgəncələrin və qeyri-insani rəftarın qarşısının alınması)	Article 10(1), 10(2) of European Convention 1950(Prevention of torture and inhuman treatment)
Azərbaycan Respublikası Konstitusiyasının24, 47, 50, 71 ci maddələri(İnsan və vətəndaş hüquq və aazadlıqlarının əsas prinsipləri 24; Fikir və söz azadlığı 47; Məlumat azadlığı 50; İnsan hüquq və azadlıqlarının təminatı 71	24, 47, 50 and 71of the Constitution of the Republic Azerbaijan (Basic principles of human and civil rights and freedoms 24; Freedom of thought and speech 47; Freedom of information 50; Guarantee of human and citizen rights and freedoms71

Bibliography

English titles

Legislation

Universal Declaration of Human Rights [1948] GA Res 217 A(III)

International Covenant on Civil and Political Rights [1948] Res 2200A(XXI), 999 UNTS 171 (entered into force 23 March 1976)

Law of Republic of Azerbaijan on Adoption of the European Social Charter 2004

European Convention 1950

Constitution of the Republic of Azerbaijan

Law on the telecommunication

Law of the Republic of Azerbaijan "On Personal Data"

"Law on Mass Media" of the Republic of Azerbaijan

Recommendation CM/Rec(2015)6 of the Committee of Ministers to the Member States on the free, transboundary flow of information on the Internet

The criminal code of the Republic of Azerbaijan

Code of Administrative Offenses

Law of Azerbaijan on the right to obtain information

Law of Azerbaijan Republic on information, informatisation and information security

Reports

Defamation and insult laws in the OSCE region: A comparative study, OSCE the Representatives of Freedom of the Media Dunja Mijatovic, March 2017

Report of Freedom House on "Freedom on the Net 2018 in Azerbaijan"

Analysis of Azerbaijani legislation on freedom of expression (Council of Europe, 2017)

Karin Karlekar, Azerbaijan, *Freedom of the Press 2010*

Legal analysis of a Single Market for the Information Society *Chapter 6: Liability of Online Intermediaries November 2009*

Books

Dominika Bychawska-Siniarska "Protecting the right to freedom of expression under the European Convention on Human Rights" published in July 2017

J.J.Carafano, "Understanding Social Networking and National Security" Joint Force Quarterly; 2011

Morgan Johansson "A national cybersecurity strategy" (2016)

Periodicals

Toby Mendel, Freedom of Expression: A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights

Alasgar Mammadli "Legal restrictions and responsibilities of freedom of expression

Digital resources

"2016 Country Reports on Human Rights Practices – Azerbaijan," U.S Department of State, March 3, 2017, <https://www.state.gov/j/drl/rls/hrrpt/2016/eur/265396.html >

Cis-legislation: Law of the Azerbaijan Republic about Personal Data <https://cis-legislation.com/document.fwx?rgn=31412>

Freedom House: Azerbaijan< http://bit.ly/KsXwTl >

European Union and Google Spain

<https://publixphere.net/i/noc/page/OI_Case_Study_European_Union_and_Google_Spain>

Facebookers, Facebook Statistics Azerbaijan, http://www.facebakers.com/countries-with-facebook/AZ/, accessed January 1, 2011

Control Over Online Sources and Facebook-like sites in Azerbaijan, Today.az, November 27, 2010, <http://www.today.az/view.php?id=77287>

Case law

Khadija Ismayilova v. Azerbaijan [2019] ECtHR

Azerbaijani titles

Legislation

Beynəlxalq insan hüquqları bəyannaməsi

Mülki və siyasi hüquqlar haqqında beynəlxaq konvensiya

Avropa Sosial Nizamnaməsinin qəbul olunmsı haqqında Qanun

Avropa Konvensiyası 1950

Azərbaycan Respublikasının Konstitusiyası

Telekommunikasiya haqqında Qanun

Kütləvi informasiya vasitələri haqqında Azərbaycan Respublikasının Qanunu

Azərbaycan Respublikasının Cinayət Məcəlləsi

Azərbaycan Respublikasının Inzibati Xətalar Məcəlləsi

Informasiya əldə etmək haqqında Azərbaycan Respublikasının Qanunu

İnformasiya, informasiyalaşma və informasiya təhlükəsziliyi haqqında Azərbaycan Respublikasının Qanunu

ELSA Bulgaria

Contributors

National Coordinator

Petar Stoilov

National Academic Coordinator

Simona Veleva LL.M., PhD

National Researchers

Vladislav Dimitrov

Ilian Antonov

Janin Al-shargabi

Gergana Urumova

Stefan Karaleev

Velislava Ruseva

Georgi Bozhidarov

Stanislav Rusinov

National Linguistic Editor

Petar Stoilov

National Academic Supervisor

Simona Veleva LL.M., PhD

Introduction

Freedom of speech is one of the cornerstones of modern democracy. Its development depends on numerous economic, social and political factors. Bulgaria's accession in the European Union in 2007 has led to many positive transformations in the country over the past 13 years. In the beginning of the membership in the EU, Bulgaria faced several legal, administrative and political challenges. However, they were promptly overcome due to the commendable preparation, the modern and well-adapted Constitution and the experience borrowed from other countries. Nevertheless, new obstacles appeared, because of the dynamic and globalized world that we live in. One of the modern challenges in front of Bulgaria is connected to the freedom of expression online. Bulgaria as a country however adapts to them and makes a legislation that is protecting the fundamental human right of expressing your thoughts freely online. Censorship is forbidden by the Constitution and is not allowed through any legal means.[300]

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

Freedom of expression is one of the fundamental values of modern democratic societies. It is secured under Article 10 of the European Convention on Human Rights which the Republic of Bulgaria has ratified. In the national legal order, freedom of expression is set forth in the Constitution of the Republic of Bulgaria. The Constitution is of particular relevance as it provides the general legal framework in accordance with which other legal acts are to be constructed. The Constitution explicitly enunciates the rights to freedom of expression,[301] freedom of press and other mediums of mass information[302] and freedom of searching, receiving and imparting information.[303] These rights are not absolute in nature and are subject to certain limitations.[304] This observation is strongly corroborated by the fact that abuse with these rights could easily cause violations of other constitutionally protected rights. A fair balance must be struck between colliding rights.

300 Simona Veleva, Evolution of freedom of speech in Bulgaria after its accession in the European Union.
301 Article 39 of the Constitution of the Republic of Bulgaria 1991.
302 Article 40 of the Constitution of the Republic of Bulgaria 1991.
303 Article 41 of the Constitution of the Republic of Bulgaria 1991.
304 Articles 39-41 of the Constitution of the Republic of Bulgaria 1991.

In the digital reality of Bulgaria, there is an abundance of examples of abusing the freedom of speech, but most frequently – concerning hate speech, dissemination of child pornography, defamation, violation of privacy, breaches of intellectual property rights and disclosure of confidential information. In order for harmful and illegitimate content on the internet to be restricted, certain censoring techniques have been introduced by the legislative among which – blocking, filtering takedown and removal of online content. Moreover, the legislation provides for the liability of internet intermediaries had a violation been found on their behalf. Taking into account the most commonly occurring violations, these measures are envisaged to protect fundamental rights as equality of dignity and rights,[305] protection of childhood,[306] inviolability of private life,[307] respect for correspondence[308] and copyrights.[309] The Constitution offers primary protection of these rights, however safeguards for them are extended and specified in other legal acts.

The Radio and Television Act is a significant source of law for safeguarding freedom of expression. It sets forth the regulation of media services and their distribution by providers under the jurisdiction of the Republic of Bulgaria.[310] The independence of providers of media services is guaranteed, however, they, in principle, bear responsibility for the choice of the content of media services.[311] Due respect is given to the protection of discrimination[312] and copyright,[313] in accordance with the framework set forth by the Constitution. The right to information is expressly addressed as a guiding principle for the providers of media services in Article 10(1).

The protection of the public interests and freedom of expression, as well as the independence of the providers of media services is entrusted to the Council for Electronic Media.[314] One of the most significant functions of this independent and specialised organ is to exercise control over the activity of media services providers, provided for in Article 32(1)(1) of the Radio and Television Act. In this way, compliance with the legal obligations arising under the same act is secured and more importantly, only legitimate content is presented to the audience.

---

305 Article 6 of the Constitution of the Republic of Bulgaria 1991.
306 Article 14 of the Constitution of the Republic of Bulgaria 1991.
307 Article 32 of the Constitution of the Republic of Bulgaria 1991.
308 Article 34 of the Constitution of the Republic of Bulgaria 1991.
309 Article 54(3) of the Constitution of the Republic of Bulgaria 1991.
310 Article 1 of the Radio and Television Act 1998.
311 Article 4 (1) and Article 5 (1) of the Radio and Television Act 1998.
312 Article 8 (1) of the Radio and Television Act 1998.
313 Article 9 (1) of the Radio and Television Act 1998.
314 Article 20(2) of the Radio and Television Act 1998.

In respect to online content, the Radio and Television Act finds application only in respect of media services for mass information.[315] Nevertheless, there are other legal sources in the Bulgarian legal order which provide for the regulation of online content. They shall be examined forthwith in the following paragraphs.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

In the Bulgarian legal system, a unified piece of legislation concretely and exhaustively covering blocking and taking down of content on the internet does not exist. The provisions addressing and regulating those censoring techniques differ and are scattered throughout the whole legislature. In this exposition, a brief review of the relevant legal acts and how they regulate the matter will be presented and a case law analysis will follow.

The systematic interpretation of the national laws regulating the means of internet censorship, namely blocking and takedown of online information, provides that they are to be seen as protective measures. The examination of their regulation in the legislature of Bulgaria will be made under the following acts: Criminal Code, Protection against Discrimination Act, Copyright and Neighbouring Rights Act, Personal Data Protection Act, Gambling Act and Consumer Protection Act.

The Criminal Code of Bulgaria stipulates that some of the aforementioned violations amount to crimes and thus are engaging the criminal responsibility of the perpetrator. Even though most of the rules were envisaged for offline implementation, they also find application online and some of them were even accommodated thereto, as is the case with the provision for distribution of pornographic material of an underage through informational technology.[316] Within this regard, Article 159(9) envisages an obligatory measure of enforcement, whereby the expropriation of the object of the criminal activity goes to the benefit of the state. In cases in which the distribution is conducted online, the material is to be deleted from its carrier or practically to be taken down. Defamation,[317] breach of correspondence[318] and discriminatory acts under Article 162(1) are also criminalised in pursuit of complying with the positive obligation of the state to create a legal framework capable of protecting

315 Article 2(1)(5) of the Radio and Television Act 1998.
316 Article 159 (2) of the Criminal Code 1968.
317 Articles 146-148 of the Criminal Code 1968.
318 Article 171 and Article 171a of the Criminal Code 1968.

constitutional rights. Intellectual property enjoys safeguards under Articles 172a – 174.

In conclusion, the Criminal Code was envisaged to provide safeguards for crimes perpetrated offline, but now also finds implementation online. It secures a wide variety of constitutional rights, especially those frequently calling for online protection by censoring instruments, however it does not prescribe an immediate opportunity to block or takedown illegal internet content. It rather enables the enforcement of obligatory measures in regard to such content. Minor breaches in respect of the Criminal Code could, in principle, be addressed in an administrative procedure.[319]

The Protection against Discrimination Act combats discrimination on any grounds established by the law.[320] Under this legislative act a Commission for Protection against Discrimination is formed and is authorised to instruct webpages to remove their discriminatory content.[321] A procedure is envisaged, whereby their decisions could be challenged before court[322] in compliance with the case law of the European Court of Human Rights.[323]

The Copyright and Neighbouring Rights Act provides for civil and administrative protection against copyright violations.[324] Together with the Criminal Code the two legislative bodies offer an overall criminal, civil and administrative protection of infringements of intellectual property rights both on- and offline.

As regards civil measures, the right to claim for compensation and a possibility to bring action before court for the destruction of unlawfully reproduced work are guaranteed under Article 95 and Article 95b(1)(3).

As to the administrative measures, the Minister of Culture or an authorised Deputy Minister has competence to exercise control over the lawfulness of collective administration of rights under Article 94sht. It also falls within the Minister's authority to order the elimination of a violation through a prescription,[325] if one is to be found.

In this legislative act, as it applies both on- and offline, blocking and taking down of illegitimate online content are again not explicitly addressed. However,

319 Article 78a of the Criminal Code 1968.
320 Article 4(1) of the Protection against Discrimination Act 2004.
321 Article 47(1) of the Protection against Discrimination Act 2004.
322 *Association Ekin v. France*, app. no. 39288/98, § 58 (ECHR, 17 July 2001); *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, app. no. 33014/05, § 55 (ECHR 5 May 2011).
323 Article 95 of the Copyright and Neighbouring Rights Act 1993.
324 Article 95 of the Copyright and Neighbouring Rights Act 1993.
325 Article 94sht (9) of the Copyright and Neighbouring Rights Act 1993.

victims of violations may seek a court order for termination. Moreover, the Minister of Culture has the authority to impose obligatory administrative measures for the same purpose.

Personal Data Protection Act enunciates the general rules for processing of personal information in Chapter Four a. In relation to takedown of content, it is an obligation of the administrator of personal data to delete and document the removal of information which was provided without a legal basis thereto.[326] Moreover, subjects of personal data have the right to require the deletion of their information when the processing is in violation of the provisions of Articles 45, 49 or 51 of the same act, or when the personal data must be deleted according to a legal obligation of the administrator.[327] The act provides for the aforementioned obligation of the administrator.[328] In this legislative body, blocking of internet content is not addressed, however takedown of information can be requested and must be implemented if there are legal grounds for it.

The Gambling Act also deals partly with internet content related to gambling. Under Article 12 of the act, the State Commission for Gambling is established. It is authorised to make decisions through which gambling games online are to be organised. Moreover, it is obliged to terminate violations and to keep a public list of eligible websites for the organisation of gambling games.[329] The publication of this list on the website of the Commission is mandatory on the day it is issued. Websites organising gambling games online, which are not included in it, must terminate the violation within three days of their notice – the date of the online publication of the list.[330] In any other case, the Commission files a request before the chairman of the Sofia District Court to decree to the providers of electronic communication networks and/or services to block the access to those webpages.[331] Although the Commission itself does not have the authority to block or takedown illegitimate content online, it may through its own motion initiate a procedure eventually leading to internet censorship.

Lastly, with the most recent amendments to the Consumer Protection Act[332] the question of blocking and takedown of content on the internet was expressly addressed. Upon violations, The Commission for the Protection of Consumers

326 Article 25a of the Personal Data Protection Act 2002.
327 Article 56 (2) of the Personal Data Protection Act 2002.
328 Article 56 (3) of the Personal Data Protection Act 2002.
329 Article 22(1)(14) of the Gambling Act 2012.
330 Article 22 (4) of the Gambling Act 2012.
331 Article 22 (4) of the Gambling Act 2012.
332 State Gazette No. 13, issued on the 14 February 2020, pages 2-7.

is authorised, pursuant to Article 190zh of the Consumer Protection Act, to issue an order, compelling:

— Traders to remove or limit the access to online interface;

— Providers of hosting services and enterprises providing public electronic communication networks and/or services to remove, block or restrict the access to an online interface;

— Registrars of domains to delete the full name of a domain when necessary and to allow re-registration when the infringement is terminated.

The Consumer Protection Act is the first legislative act to expressly address blocking and takedown of internet content and to authorize the immediate implementation of those measures by administrative authorities.

Recently, the European Court of Human Rights, hereinafter - the ECtHR, delivered its judgment on the case of *Pendov v. Bulgaria*, app. no. 44229/11,[333] which concerns the right to the peaceful enjoyment of possessions under Article 1 of Protocol 1 and the freedom of expression under Article of the European Convention on Human Rights (the Convention). The principal facts of the case could be summarised as follows - a publishing house complained, pursuant to Article 172a of the Criminal Code, that a book published by it had been made available on Internet, more precisely, on a site partially hosted on a server owned by Lazar Milkov Pendov (the applicant). The police, authorised by a search warrant, seized the server on which, additionally to the aforementioned, a site belonging to the applicant was hosted. The applicant opted for filing several requests, in accordance with Article 111 of the Criminal Code, to the respective authorities in order for his property to be returned to him. The server was returned to him after more than 7 months. Nonetheless, the applicant lodged a complaint before the ECtHR in respect of the alleged violations of his rights secured under Articles 10 and 1 of Protocol 1.

The ECtHR noted that the complaints under the aforementioned Articles are neither manifestly ill-founded, nor inadmissible on any other grounds. Therefore, it proceeded to examine them on the merits.

With regard to Article 1 of Protocol 1, the ECtHR found that the seizure of the applicant's server was lawful and pursued a legitimate aim, namely - for the prevention and disorder of crime and for the protection of rights and freedoms of others.[334] The pertinent question was whether the measure was proportionate.

333 *Pendov v. Bulgaria* app. no. 44229/11 (ECHR).
334 *Pendov v. Bulgaria*, app. no. 44229/11, § 43.

The ECtHR, taking into consideration the conduct of the relevant authorities, the necessity of the measure, the length of the retention of the applicant's property and the consequences for him, concluded the seizure was disproportionate. In particular, the ECHR noted that the interference was unjustified mainly due to the inactivity of the authorities in respect of the request of the applicant, the absence of examination of the server for the purposes of the investigation and the importance of the server for the professional activity of the applicant.[335] Therefore, there was a violation of Article 1 of Protocol 1.

In respect of Article 10 of the Convention, the ECHR noted that the freedom of expression applies 'not only to the content of information, but also to the means of dissemination, since any restriction imposed on the latter necessarily interferes with the right to receive and impart information.'[336]

Turning to its reasoning under Article 1 of Protocol 1, as the claims under both Article 10 and Article 1 of Protocol stemmed from the same fact, the ECtHR found that the interference was unjustified and disproportionate to the right secured under Article 10 of the Convention. In particular, the ECtHR pointed out that the retention of the server during the criminal proceedings proved to be unnecessary for the purposes of the investigation and for a period of time the relevant authorities made little to no effort in order to remedy the effects of their actions on the applicant's freedom of expression.[337] Accordingly, there has been a violation of the freedom of expression.

In conclusion, although the freedom of expression, including online, may be subject to interferences, as provided for both in the Convention and in the Constitution of the Republic of Bulgaria, in order for such an interference to be justified, it must be in accordance with the law and in pursuit of a legitimate aim. Moreover, due care shall be afforded by the authorities within whose competence the termination of an interference with the freedom of expression falls. Only in this scenario, the balance between the freedom of expression and other rights will be calibrated to the extent expected in a democratic society.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

Bulgarian legislature outlines a number of mechanisms that may affect illegal content and lead to its blocking, filtering or taking down. The mechanisms are

335 *Pendov v. Bulgaria*, app. no. 44229/11, § 50.
336 *Pendov v. Bulgaria*, app. no. 44229/11, § 53.
337 *Pendov v. Bulgaria*, app. no. 44229/11, § 66.

based on the Constitution of the Republic of Bulgaria and all provisions of international covenants and conventions ratified and in effect as part of the legal framework in the country. The establishment of an explicit legal framework as opposed to a case-by-case assessment is understood to pose a threat of undue censorship by the Bulgarian legal system.[338]

Thus, the legal mechanisms outlined by the national legislator are as follows:[339]

- The Constitution of the Republic of Bulgaria (CRB) and the practice of the Constitutional Court (CC) reinforce the practise of case-by-case assessment of the balance of freedom of speech and regulation of content that may be harmful to society or the individual;
- The restriction of certain rights is subject to Criminal Code provisions, some of which, but not limited to:
- Restriction of pornographic material (Article 159, Paragraph 2 of the Criminal Code);
- Restriction of online crimes of private nature - insult (Article 146 and Article 148 of the Criminal Code) and defamation (Article 147 of the Criminal Code).
- Removal of copyright content that has been unlawfully distributed - Article 96 of the Copyright and Neighbouring Rights Act (CNRA) and Article 172a of the Criminal Code;
- Hate speech is regulated by Article 4 of the Law on Protection from Discrimination (LPFD);
- The Law for Protection of Personal Data regulates the unlawful distribution of private information;
- The Law on the Ministry of Interior, the Law on the State Agency 'National Security' (SANS) and the Criminal Procedure Code also contain institutes that can lead to the blocking or removal of unlawful and harmful online content;

338 Comments of Bulgaria on the country report of the Comparative study on blocking, filtering and take-down of illegal Internet content, page 1.

339 Comments of Bulgaria on the country report of the Comparative study on blocking, filtering and take-down of illegal Internet content, page 1-2.

— Since 2015 the practice of voluntary blocking can also be found through the signing of memorandums between Internet providers and local authorities.

Furthermore, the Swiss Institute of Comparative Law lists other mechanisms in their study 'Blocking, filtering and take-down of illegal internet content':[340]

— The Gambling Act penalises gambling sites that do lack the mandatory license for such activities;

— However, they find the lack of specific regulation concerning the press and electronic media problematic.

The Bulgarian legislature at times does not distinguish filtering as something different than blocking.[341]

Blocking of sites can be on the legal grounds of a court decision, such as the procedure in cases where the Gambling Act has been breached.

Such a case was brought forward before the District Court of Kardzhali (case № 882/2013, 26 November 2013). The facts were as following: Y.Y. questioned the legality of a penal decree № 13/2013 from 10 June 2013 from the Chair of the National Gambling Commission. He was penalised for using an online site 'betuniq.com' to place bets and orchestrated gambling games. The plaintiff claimed there was a lack of clear evidence as well as reasoning given for the issuing of a penal decree. The court considered all testimonies given by the witnesses and upheld the penal decree which fined Y.Y. for an amount of 5000lv and confiscated his computer technology. This case and similar other show that a common practice is taking away the incriminated technology as a means to cut his access to his illegal activities.

Chief Directorate Combating Organised Crime of the Ministry of Interior is the competent authority in the combating of illegal activities and crimes with high public endangerment. It carries out investigations and research in cases, connected to pornography, terrorist, online abuse and such topics. In accordance with the Ministry of Interior Act, article 64 police bodies can take measures to eliminate 'grounds for the incidence of crime and other violations.' Similar power is given to the State Agency for National Security through the

340 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015.

341 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 112.

State Agency for National Security Act. These government bodies can issue written instructions to internet providers to block illegal content.[342]

Such an instance was when the site motikarq.com was taken down by the Chief Directorate Combating Organised Crime. The site was known to contain child pornography, blackmail minors for more elicit content and some illegal financial operations.

The Chairman of the Consumer Protection Commission can also issue written instructions for the blocking of illegal content, in accordance with the Electronic Commerce Act. The Commission against Discrimination has the power to restrict discriminatory online content, in accordance with the Protection against Discrimination Act.[343]

Furthermore, people affected by a breach of their rights can submit a request for the removal of harmful content to the Internet Service Provider (ISP). If there is a dispute about the illicit nature of the content, the case may be brought to court. Court decisions concerning the blocking or removal of online content then are motivated and communicated under the Civil Procedure Code. These decisions can be appealed before the Appellate Court, and at the next level before the Supreme Court of Cassation.[344]

The ISP may be liable for tort under civil legislation and if its behaviour represents criminal activity it will be criminally liable. If the ISP is prosecuted under the Criminal Code, then in power comes the Criminal Procedure Code.[345]

Such an instance was brought forward before the District Court of Sofia(№ 2996/2017, 15 November 2018) by F.P.H.P, who claimed that a company by the name of R. Ltd. sold, distributed and advertised replicas of clothing products, under the distribution license of F.P.H.P. The facts showed that the owner of the site did not post the advertisements for the products, they were made and managed by third-parties, there is a mechanism to forward complaints towards the site and after their overview posts can be taken down, there had been correspondence between the plaintiff and defendant on account of the replicas of products on the site, there had still been posts with replicas during the moment of the court process, the defendant had had an active role in the

342 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 113 and 114.

343 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 114.

344 'The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 114 and 115.

345 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 119.

promotion of the products and had received information on purchases through postal services and given customers points based on the carried out purchases. The court's decision was that the defendant is responsible for being compliant with the selling of replicas because he had had an active part in the process between the buyers and sellers, due to the policies of the site - advertisement and point distribution, also the defendant had taken an active role in overlooking the content on his site, there were instances where posts concerning electronic devices were taken down, due to the suspicion of inauthenticity, the court argues that such an active role should be taken in relation to posts concerning clothing and other products as well, as opposed to the passive role taken in the case in question, the defendant was considered to have had the viable resources to restrict the posts and was convicted to take down the posts. This decision shows that the law provides a working mechanism to hold sites accountable for their content. It also provides criteria when the sites are liable, even if the seller of a product is a third-party: the owner of the site has to have a role in the purchasing process, as opposed to being neutral, in the given instance the owner helped with the advertisement and knew of the purchases taking place.

When the blocking is motivated through specific laws like the Gambling Act or similar, the appeals are brought before the Administrative Court.[346]

There is no official organ that overlooks online content. This is carried out through ISPs through their terms and conditions and moderators. Moderators can delete or hide opinions that have spam, racist, sexist or xenophobic content. This leads to the main mechanism of combating harmful online content to be self-regulation. An alternative measure for victims of online abuse can be alerting the authorities on the grounds of the relevant legislature and bringing forth the issue in court.[347]

The self-regulation sites carry out has risen since the Delfi vs Estonia case, which obligated media sites to moderate the comments under their articles. On the grounds of the decision of the ECtHR, the Supreme Administrative Court of Bulgaria confirmed the obligation of sites to regulate their comment sections and to censor offensive content in comments in its ruling in case № 10756/2015 from 12 December 2016, which concerned the appeal of a media site btv.bg against the decision of the Commission against Discrimination.

346 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 119.

347 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 119 and 120.

The overall consensus is that the legislature that exists is not coherent, nor precise, it has a difference in terminology and a mix of old and new laws. There is also no consistent case law as a source of practice.[348]

The framework in Bulgaria seems as if it is compliant with the human rights standards and the decisions and developments in the ECtHR and its practice.

The Constitution guarantees basic rights. In Decision № 7/1996 of the Constitutional Court judges speak about the communications rights and freedoms of citizens and the Administrative Procedure Code has articles that reinforce the principle of proportionality that can safeguard the freedom of expression when in conflict with other rights of the individual. Still there is a lack of overall understanding of the issue, this diminishes the power that a culture of independence, experts and civil society can have as a safeguard.[349]

A specific instance of a breach of the rights of the individual was the case of a Facebook group that was in support of Laura Koveci, where individuals also posted critical material towards the Bulgarian government. There were instances where the posts were taken down and the admins of the group were blocked. Evidence concerning who was behind the restrictions pointed towards the State Agency for National Security. One of the admins contacted the Facebook Headquarters, where experts proceeded to fix the issues the admin faced. This points towards the lack of clear a process of assessment and the lack of information towards citizens on how to understand why a post has been deemed as problematic and what actions can be taken to question its takedown.

In such cases, individuals that feel that their right of expression has been breached can bring forth a case before the Bulgarian court. This leads us to believe the legal framework does provide means of protection that can help uphold the right of expression.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

There are few regulations in Bulgaria concerned specifically with Internet censorship, rather, the area is governed by general legislation concerning censorship and the freedom of expression. Thus, the development of self-regulation of blocking and taking down of content in the private sector is

348 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 122.

349 'The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 124.

supplementing the relative lack of regulations. We will look into examples of the development of soft law, the use of arbitration and moderation, with relevant examples in the fields of online media, public forums and disputes of domain names in the .bg zone. The examples have been chosen on the basis of them being cases of self-regulation on the national level in Bulgaria.

The general issue of the self-regulation model is that it has led to the over-removal of content so as to avoid risks, which constitutes a human rights problem in some countries.[350] However, this seems not to be the case in Bulgaria, perhaps due to the incomplete development of self-regulation tools, which leads to cases of hate speech in articles of online media and forums. The lack of self-regulation in this area however is far from the only factor, influencing these displays. If anything, it can positively influence these processes, when applied correctly and effectively and when a balance has been struck between the freedom of expression online and protecting the rights of others.

There is a lack of specialised regulation concerning online media, so it is subject to the provision of general legislation. The existing Radio and Television Act regulates media providers, but not the circulation of content on the Internet. The existing Council for Electronic Media also does not control online content. The need to uphold the standards of free and trustworthy journalism has led to the creation of the Ethical Code of Bulgarian media in 2004, together with the Commission of Journalistic Ethics.[351] The Commission for Journalistic Ethics can direct non-binding recommendations on any type of materials published by press, electronic and online media. This makes the Commission the only self-regulatory body, which can impose restrictions on the online media outlets, which are otherwise unrestricted. However, not all media outlets have joined the Ethical code. Furthermore, other commissions exist, and other Ethical codes are also applied for different media groups.[352] This has led to the fragmentation and fairly limited impact it has played on the media landscape. Most of the complaints which are brought to the Commission for Journalistic Ethics are connected with misrepresenting information, inciting discrimination[353] and other issues. On several occasions the Commission has recommended that the 'online

350 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 29.

351 National Council for Journalism Ethics, 'Code of Ethics of the Bulgarian media' <https://mediaethics-bg.org/%d0%b5%d1%82%d0%b8%d1%87%d0%b5%d0%bd-%d0%ba%d0%be%d0%b4%d0%b5%d0%ba%d1%81-2/> accessed 18 February 2020.

352 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 120.

353 Decision of Commission of Journalistic Ethics №25, 12/07/2016.

media should make efforts to not to allow any form of hate speech in the reader's fora.'[354]

Overall this model of self-regulation has not been proven to be effective due to the non-binding nature of the Ethics Commission's decisions and the large number of media outlets that do not abide by its rules. Consequently, the system has not greatly contributed to the takedown of hateful and defamatory content and for generally improving the state of the media landscape, for which judicial protection remains the only means for redressing grievances.

When it comes to the current state of the media landscape in Bulgaria, the problems are of a wide spectrum and are subject to various interdisciplinary studies- journalistic, economical. political, etc. Concerning the legal issues, one could say that in general the problems lie not within the blocking, take down of content and legal censorship on behalf of the state, but are rather connected with the general poor quality of some media outlets, political pressure of Bulgarian officials towards the opposition media (de facto censorship), non-transparency of the ownership of media outlets both on and offline and others.[355]

The case for battling the spread of hate speech can be examined both from the point of view of media publications, as well as from the position of online forums, which are a key factor in a free and pluralistic media environment. That is why it is very important to take a look at the developments in the area of forum moderation. In June of 2015 the case of the ECtHR Grand Chamber of *Delfi AS v. Estonia* came out.[356] In summary, the case ruled that websites should actively monitor their online forums for illegal comments and that they carry liability for them. This sparked a wave of debates among some Bulgarian news websites and forums, with some pointing out that this would most likely lead to more auto censorship and ultimately to a demise of the quality of free speech. However, other analysts saw the case as an opportunity to raise the quality of debate in the Bulgarian media landscape.[357] The aftermath of the case is that five years later most serious online news sites in Bulgaria have more stringent requirements in their comment sections; there are moderators, who can take down content and only registered users are able to publish comments. This has allowed the level of debate in the forums to become more civilised, in spite of

354 Decision №15 31/05/2016 of the Commission for Journalistic Ethics.

355 Annual Human Rights Report for 2018 by Bulgarian Helsinki Committee, page 57.

356 Case of *Delfi.AS v. Estonia*, European Court of Human Rights, Grand Chamber, Application no. 64569/09, 16/06/2015.

357 Media law expert professor Nelly Ognyanova commenting on the different opinions (in Bulgarian).

initial reactions of media websites blocking their comment section in fear of being sued.[358]

In general, the moderators of comment sections will remove comments if they do not meet the guidelines, which have been set out by the websites themselves. For example, the user policy for the comment sections of Economedia group editions (featuring online news websites such as 'Capital' and 'Dnevnik') states that comments will be removed by moderators if they contain 'spam, obscene or vulgar expressions, racial, sexual, ethnic or religious abuse, offensive descriptions of the physical, intellectual or moral qualities of particular persons, incl. to other forum participants'[359] as well as 'personal data protected under the Personal Data Protection Act and content entirely in a foreign language'.[360] The reporting of comments by users will accelerate this process of moderation and eventual blocking. This model is generally applied throughout the different forum sections of online media and has proven to be effective.

Another example of self-regulation concerning the take down of content, although in a narrow, but important field of Internet regulations, is the procedure for arbitration in the occurrence of disputes concerning domain names in the .bg zone (the domain for Bulgarian websites). The Bulgarian domains are administered by a Joint Stock Company called IMENA.BG.[361] The organization, called a registry, has been delegated the rights to register the names in the .bg zone. The customers, called registrants, apply and get their domain names registered by the register (IMENA.BG in this case). The domain name can be either protected or unprotected. A protected domain name is one for which documents have been presented during the registration by the REGISTRANT, certifying grounds to use the LABEL according to the Terms and Conditions.[362] This way a company can protect their domain name in a case of a dispute. The procedure of the dispute is prescribed in the Terms and conditions for domain name registration and support in the .bg zone and the sub-zones[363] - establishing the right of prior tempore, potior iure (Whoever is earlier in time is stronger in right). When a dispute is filed for arbitration, a

358 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page 120.

359 User policy for Economedia forums (in Bulgarian) <https://www.economedia.bg/forum.php> accessed 20 February 2020.

360 ibid.

361 The register of names in the .bg district <https://www.imena.bg/tld_user_nam/app.pl?action_key=ac_c1p2d1_to_about_us&frame_key=fr_c1p2_main_frame> accessed 20 February 2020.

362 Terms and Conditions for Domain Name Registration and Support in the .Bg Zone and the Sub-Zones <https://www.register.bg/tld_user_reg/documents/en/terms_and_conditions-v4.9.pdf> accessed 20 February 2020.

363 ibid.

committee is formed in order to solve it. If the dispute is solved in favour of the claimant, the losing side has its domain terminated, unless within this period the REGISTRY does not receive a protective order by a Bulgarian competent court, by which the 'stop the domain name termination' protective order has been applied to the registrant.[364] There are also provisions in the cases of municipality names and protected landmarks.

Even though the process of arbitrating disputes in the area of domain names is a very particular procedure, it shows that in some areas of the private sector, questions connected to the takedown of content can be left to self-regulation, while still having the possibility to turn to court if necessary.

To sum up, the private sector in Bulgaria has not fully implemented the possibilities of applying self-regulation in a way that could benefit itself and the users of different Internet platforms or services. It is notable that Bulgaria does not face most of the issues that other countries have experienced when it comes to applying self-regulations in the private sector e.g. the over-removal of content, leading to limiting the freedom of expression. Even the *Delfi AS v. Estonia* case, which some argued would be damaging to free speech, has actually contributed to some degree for the improvement of quality and civility of debates in the forums of most online media. However, other instances of applying self-regulation, such as the Commission for Journalistic Ethics have not been as effective, but that has also been caused by the fragmentation and the incomplete participation of all media outlets.

In conclusion, the field of self-regulation still has ways in which to develop, but it should be in a manner that guarantees the rights of others does not infringe on the freedom of expression online.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

25 years ago, on 13 December 1995 Directive 95/46/EC on the protection of individuals concerning the processing and free movement of personal data (hereinafter referred to as Data Protection Directive or DPD) came into force. The provision of Article 12(b) of the aforementioned Directive refers to the right to access and reads that 'Member States shall guarantee every data subject the right to obtain from the controller […] the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this

364 ibid.

Directive.' Furthermore, data subjects also had the right to obtain from the controller notification of any rectification, erasure or blocking to third parties to whom the data have been disclosed.[365] Thus, the Right of Erasure, more commonly known as the right to be forgotten, was already established in the DPD. However, the massive development of communication and information technology in recent years indicated a modernisation of the legal framework of personal data protection at the European level. The scale of the collection and sharing of personal data has increased significantly,[366] which led to adopting the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data or the General Data Protection Regulation (hereinafter referred as GDPR), and repealing Directive 95/46/EC. Its provisions became directly applicable in all member states on 25 May 2018.

One specific right of the data subject which gained prominence after the adoption of the GDPR was namely the right to erasure, enshrined in Article 17 of the Regulation. Bulgaria, as a Member State, is obliged to comply with the provisions of the respective Article. According to Article 17, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay under certain conditions. These circumstances are comprehensively regulated in Article 17, paragraph 1 and read as follows: 'where the data is no longer necessary in relation to the purposes for which it was collected, where the data subject withdraws consent on which the processing of personal data is based or raises a legitimate objection to it, where the processing of the personal data has been done in an unlawful way, where the data controller is a subject to a certain legal obligation and where the controller offered information society services directly to a child in relation to Paragraph 1 of Article 8.'

Paragraph 2 of the same Article reinforces the previously established subject's right of access in accordance with Recital 66 of the GDPR. Recital 66 states that 'To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to or copies or replications of

365 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23 November 1995, Article 12, point 3.

366 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 6.

those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.'[367] It obligates the controller to inform other controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of those personal data, in case the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase it. The personal data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures to ensure the erasure in its entirety. The right to be forgotten, however, is not an absolute right – there are several exceptions where the processing of sensitive personal data is prohibited. The right of freedom of expression and information is the first legitimate argument that GDPR defines as an exception of the right to be forgotten. This gives the data controllers the right to reject some claims based on the right to erasure if exercising the right of freedom of expression and information would be jeopardised in that context.

Protection of expression and information rights also appears to be the mainspring of the few examples of interpretation and expressed position of the Bulgarian authorities in relation to the right to be forgotten. The current legislative framework at the national level has been adopted in such a way as to incorporate elements of the GDPR in accordance with Principle 10 of the Regulation. However, the provisions in relation to the right to delete are considered recent, having been implemented in the penultimate amendment of the Personal Data Protection Act from 26 February 2019.[368] As a result of the recent entry into force of the aforementioned legal arrangements in relation to the right to erasure, the judiciary has not yet ruled on the matter and both legal theory and practice have not yet generated conclusive insights in the field as well. The results of the analysis of Bulgarian legislation and relevant jurisprudence can certainly show that the legal term 'right to be forgotten' does not exist in the current legislation. Although the concept of the right to be forgotten is not legally defined under Bulgarian law, the main legal provisions of Article 17 of the GDPR are additionally laid down in the Bulgarian 'Personal Data Protection Act'. In particular, paragraph 2 of Article 56 of the law indicates the different grounds for obtaining the right to erasure of the data subject's data. It stipulates, that the data subject shall have the right to obtain from the controller the erasure

367 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23.11.1995, Article 12, point 3.

368 State Gazette №17 of 2019.

of personal data concerning him or her where the processing infringes the provisions of three other articles from the same law (Article 45, 49 or 51) or where the personal data have to be erased for compliance with a legal obligation of the controller.

Article 45 for its part expressly lays down the conditions under which personal data must be processed. Uppermost, under point 1 of paragraph 1 of Article 45, personal data must be processed lawfully and in good faith. The second point of paragraph 1 sets out that the data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Personal data shall also be adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed, according to point 3 of the same paragraph. Furthermore, it is required that it is accurate and, where necessary, kept up to date; every requisite step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[369] Regarding the storage period of the personal data, point 5 stipulates that the data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the said data are processed. Lastly, point 6 provides that the personal data should be processed in a manner that ensures appropriate security of it, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures. The data controller is obliged to reply to every request of the data subject, including requests in relation to his or her right to delete, within a certain period of time – two months of receipt of the request. The controller could also inform the said subject in writing of the action taken on the request within the prescribed period. That period may be extended by one further month where necessary, taking into account the complexity and number of requests.[370]

In order for the processing to be lawful, it shall also comply with the provisions of Article 49 of the present law. According to Article 49, one condition, under which the processing of personal data shall be lawful is where it is necessary for the exercise of powers by a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of, threats to public order and security. Another context, which Article 49 regulates is where the processing is provided in Union law or in a

369 Article 45, paragraph 1, point 4 of the Personal Data Protection Act.
370 ibid, Article 53, paragraph 3.

statutory instrument that defines the purposes of the processing and the categories of personal data that are processed.

Similar to Article 9 of the GDPR,[371] Article 51 of the Personal Data Protection Act also regulates the processing of special categories of personal data. Although this right is not absolute and there are certain cases where data of this nature shall be processed, it is pertinent to note that Article 51 has rather broadened the scope of those exemptions in comparison to Article 9 of the GDPR. It essentially regulates grounds for allowance of processing of personal data of such special categories. According to paragraph 1 of Article 51, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed where this is strictly necessary, there are appropriate safeguards for the rights and freedoms of the data subject and is provided for in Union law or the legislation of the Republic of Bulgaria. Paragraph 2 of the Article stipulates that 'where processing under Paragraph 1 is not provided for in Union law or the legislation of the Republic of Bulgaria, the data referred to in paragraph 1 may be processed where this is strictly necessary, there are appropriate safeguards for the rights and freedoms of the data subject, and the processing is necessary to protect the vital interests of the data subject or another natural person, or if the processing relates to data which are manifestly made public by the data subject.' Paragraph 3 implies that suitable measures and safeguards for non-discrimination against natural persons shall be put in place where data under paragraph 1 are processed, in compliance with Principle 71 of the GDPR.

The Bulgarian Commission for Personal Data Protection (CPDP), established in 2002, is the supervisory authority at a national level, responsible for the protection of personal data.[372] With regard to the implementation of the right to be forgotten, the Commission has published an opinion on the application of the right to be forgotten in the context of personal data processing for journalistic purposes in April 2019.[373] The opinion follows the extensive public

371 According to Article 9 of the GDPR, 'Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.'

372 Article 1(4) point 1 of the Personal Data Protection Act.

373 Commission for Personal Data Protection, Opinion on the application of the right to be forgotten in the context of personal data processing for journalistic purposes, <https://www.cpdp.bg/index.php?p=element_view&aid=2183> accessed 25 May 2020.

discussions and intense media opposition in Bulgaria against several assessment criteria for the processing of personal data for journalistic purposes and purposes of academic, artistic, or literary expression (Article 85 of the GDPR). Some criteria are, for example, the impact that the disclosure of the personal data or the publishing of the data would have on the data subject's privacy and reputation, the type of the data processed and the circumstances under which the personal data became known to the controller. The President of the Republic of Bulgaria, Rumen Radev, issued a motion vetoing the aforementioned provisions, arguing that they would lead to overregulation and misbalance between the right to protection of personal data and the right to freedom of expression and information. Nevertheless, the law was promulgated in the State Gazette on 26 February 2019, but nine months after the Personal Data Protection Act was gazetted, the Bulgarian Constitutional Court declared the provisions as contradictory to the Constitution of the Republic of Bulgaria and, hence, invalidated them.[374]

In its opinion, the commission in the first place makes reference to the judgement of the Court of Justice of the European Union in Case C-131/12 (Google-Spain decision),[375] aimed at clarifying a number of very important issues relating to the right of data subjects to be forgotten. The commission expresses that the decision of the CJEU on the Google-Spain case is a precondition for striking a fair balance between the right to privacy and the protection of personal data of individuals, freedom of expression, right of access to information and other legitimate interests of individuals on the Internet. The CPDP expressly emphasises that the right of protection of personal data is not an absolute right ab initio, it shall be applied considering its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality, as per Principle 4 of the GDPR. In this regard, given that the controller is exercising the right of freedom of expression and freedom of information, including for journalistic purposes, the request for the erasure of personal data can be refused. The Commission substantiates its position, writing that essential activities for journalism are the collection, analysis, interpretation and dissemination by the mass media of topical and, most importantly, publicly relevant information. Restriction of freedom of expression and information is permissible only insofar as is necessary in a democratic society under paragraph 2 of Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. As regards the specific case which gave rise to the

374 Court Decision № 8 of 15 November 2019 under Constitutional Case 4/2019.

375 Judgment of the Court (Grand Chamber), 13 May 2014. *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos* (AEPD) and Mario Costeja González, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN> accessed 20 February 2020.

publishing of the CPDP's opinion, that case concerned the requests for exercising the right of erasure by a particular individual that some media outlets have received. The aforementioned media have published articles about him regarding his conviction with a final verdict, hence, he wanted to exercise his right to be forgotten. Undoubtedly, the dissemination of information related to the commission of crimes, as in the current case, constitutes journalistic activity. The task of the media, and in particular the journalists, is to provide transparency and information to citizens, helping to protect the public interest. According to the commission, the disclosure of information about criminal offenses committed by a convicted person is in favour of the society, thus helping to achieve the goals of general prevention as an element of the state's criminal policy. What is more, it encourages citizens to be more vigilant so that they do not become victims of similar types of crime in the future. The commission further notes that in the context of criminal proceedings, all facts and personal data relating to them have become publicly available with the delivery of the final verdict. In relation to the term for disclosing journalistic information containing personal data, the opinion of the commission reads that it should comply with the storage limitation principle, set out in Article 5 of the GDPR. That is to say, the personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In the light of the aforementioned arguments, journalists may ignore requests to delete convicts' personal data in the context of journalistic purposes, which essentially restraints a convicts' right to erasure.

6. How does your country regulate the liability of internet intermediaries?

The problem with the liability of internet intermediaries is expressly addressed in the Electronic Commerce Act. This legal act sets out the general framework for the liability borne by internet service providers. As there is no other legislative body providing for the responsibility of internet intermediaries, the provisions of the Electronic Commerce Act are applied by analogy in situations falling outside of its scope. Chapter Four of the act envisages situations in which the civil liability of internet service providers may be engaged.[376] Internet service providers must comply with their positive obligations, as well as to abstain from certain behaviour (negative obligations). Redress for damages directly resulting from non-compliance with the obligations of internet intermediaries could be

[376] Article 13-18 of the Electronic Commerce Act 2006.

filed by affected natural and legal persons alike. Following the systematic structure of the relevant provisions set out in the act, this exposition will describe how the liability of internet intermediaries is regulated and what obligations do service providers have.

Article 13 of the Electronic Commerce Act stipulates the conditions for engaging the liability of internet service providers when providing services for access and transmission. Internet service providers bear no responsibility for the content of the information and for the activity of the receiver when they do not engage in:

— initiating the delivery of information;

— choosing the receiver;

— choosing or amending the information provided.

However, when internet service providers are actively engaged in processing of information, they shall bear responsibility.

Article 14 of the Electronic Commerce Act covers the liability for services for automatic search for information. Under this Article, upon compliance with the negative obligations enunciated above, the provider of services for automatic search of information does not answer for the content of the information gathered by the consumer. However, if the provider or a natural/legal person connected to him is the owner of the informational resource from which information was extracted, then the provider shall bear objective liability.[377]

Intermediate storage or caching is addressed in Article 15.[378] The term "caching" must be understood as the automatic, intermediate and temporary storage of information, especially when needed for the effective transmission to the consumer upon their request. The provision imposes both negative and positive obligations upon compliance with which the internet service providers can evade liability. The negative obligation is to abstain from modifying or amending the information. The positive obligations encompass compliance with the requirements for access to information and the generally accepted rules governing updates of information. In addition, providers are obliged to lawfully make use of the generally accepted instruments for receiving data and also to immediately remove or stop the access to stored information upon taking notice of:

377 Article 14 (2) of the Electronic Commerce Act 2006.
378 Article 15 of the Electronic Commerce Act 2006.

— the lack of access to or the removal of the information by its initial source;

— the presence of an order by a competent authority stipulating the removal or the block of access to the impugned information.

Internet service providers must act in an expeditious manner when removing information or disabling access thereto. However, when the publication of information amounts to a crime, they must restrict the access to it and preserve it as electronic evidence.[379] In any other case, internet service providers will bear criminal responsibility under Article 294 of the Criminal Code.

Article 15 of the Electronic Commerce Act is the first instance in which the legislature provides that blocking and takedown of internet content are to be interpreted as positive obligations of internet service providers.

With regard to the liability for hosting and linking, Article 16 of the Electronic Commerce Act stipulates that internet service providers shall not be held accountable, if they did not know about the unlawfulness of the content or of the activities of the receiver. Moreover, they are not to be held liable, when the circumstances in respect of which the content or the activities of the receiver were obviously unlawful had not come to their knowledge.[380] However, these provisions do not apply when the receiver and the provider are connected. Further, when it has come to the attention of the provider that the content or the activities of the receiver were unlawful and the provider did not take adequate measures (blocking, takedown, etc.), the provider is liable.[381] Moreover, in this case, they are obliged to preserve the information, if it is provided for in the law. Under Article 16(3), internet service providers are under the legal obligation to provide any information concerning the receiver and their activities upon request from a competent state authority.

Lastly, it is notable that internet service providers are not required to observe and examine the information which they store, transmit or make accessible.[382]

In conclusion, the liability of internet intermediaries is almost exclusively regulated under the provisions of the Electronic Commerce Act. Although this act provides only for the civil liability of internet service providers, this fact does not preclude the engagement of criminal liability when there are legal grounds to that end. Internet service providers are generally not responsible for the

379 Article 159 of the Criminal Procedure Code 2005.
380 Article 16(1) and (2) of the Electronic Commerce Act.
381 Article 16(2) of the Electronic Commerce Act.
382 Article 17 of the Electronic Commerce Act 2006.

content they are providing, however, it is expected of them to demonstrate due care in order for their civil liability not to be invoked.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Taking into account the analysis so far, the recommendations and policies of the European Union, the political programme of the Council of Ministers, the most recent amendments in the relevant legislative acts, as well as the general tendencies in the advance of legislation concerning this topic, one could make a prediction of the forthcoming developments over the next five years in Bulgaria. In the area of online blocking, take down and filter, for example, one of the issues that exist now is the lack of government-regulated information and access to knowledge how one can protect their right to expression or alert authorities of illegal content. The authors of this report believe that in the near future the government will sanction mandatory access to public information through legislative effort. There are already classes for cybersecurity in school and obligations for sites to inform users for their rights over their personal data, we believe such measures can be used to inform users on online censorship as well. On the international level, the development of EU law and the practice of the ECtHR will also influence Bulgaria's national legislation and jurisdiction in the area of online censorship. Furthermore, with the rise of online censorship issues, we predict that more people will be affected and will seek their rights in court. This will lead to more national practice and may bring a more unified approach toward the issue, as opposed to the current state, which consists of a lack of data and contradictory points of view on certain aspects. We believe that legislature will become clearer and more precise when addressing these issues, as now there are instances where certain definitions are seen as interchangeable, even though they address different issues (i.e. filtering and blocking). Perhaps a single institution, overlooking all of these issued will not be established, rather the individual organs will face changes to their structure and will become more specialized in their area of expertise (Commission against Discrimination, SANS etc). Finally, when it comes to self-regulation, online platforms in general will become more aware of their obligation to restrict illegal content that may be posted by third-parties, because of the prospect of being held liable.

Bulgaria, as a member state of the European Union, is bound by the legislative acts adopted by the European Union. Whether they would take the form of a directive or a regulation, they must be incorporated appropriately in the national legal system. To that end, the latest amendments to the Personal Data Protection Act reflect the influence of European legislature on the Bulgarian legal order. Concerning "the right to be forgotten", as evident from the current national legislative framework, Bulgarian legislation implements to a large degree the legal principles and provisions at a European level successfully. Looking forward, particularly into the next couple of years, the Bulgarian Commission for Personal Data Protection developed a strategy for improvement in the area of personal data protection, which underlies the commission's long-term operation. In the SWOT analysis of the Horizon 2022 strategy,[383] the Commission identified the limited financial resources (budget and salaries), the small staff size and high rate of labour turnover and the insufficient number of IT experts in the CPDP administration who are narrowly specialised in the field of personal data protection as some of the weaknesses in the sector that need to be overcome. However, with respect to the potential opportunities, the strategy states that the forthcoming modernisation of the national legal framework will make it possible to remedy the weaknesses committed so far. Furthermore, the commission should carry out standardising good practices in the separate areas and activities of the commission, by setting up a national training centre in personal data protection for instance. The commission shall also broaden its opportunities for external financing, deepen the cooperation with the non-governmental sector and the academic community and build a system for obtaining regular feedback from a large number of stakeholders. Enhanced participation in initiatives, forums and entities at both EU and international level and steady improvement and enhancement of the level of satisfaction of citizens, organisations and partners with the services provided are considered as a priority matter as well.

Considering the most recent controversies with Facebook, a greater level of data protection will be sought. It is only logical to suggest that more stringent requirements will be imposed on internet intermediaries in the future, while broader possibilities will be granted for takedown and blocking of illegitimate content online. The Bulgarian legislation will follow accordingly.

Regarding the aims set out in the programme of the Council of Ministers, the executive is aiming for the effective prevention of crime. This includes crimes perpetrated online, e.g. child pornography. The current practice in criminal legislation does not indicate that an immediate opportunity to block or take

383 Strategy Horizon for 2022, published by the Commission for Personal Data Protection.

down information will be provided for. However, with the development of the future strategy for criminal policy, it is to be expected that the executive agencies will be authorised to intervene more actively in order to remedy possible violations. Moreover, taking into account the breach of the data archives of the National Revenue Agency, it may be reasonably concluded that in the next 5 years the required level of protection of personal data will be raised and thus intermediaries in non-compliance will be subject to harsher sanctions.

The positive tendency shown in the most recent amendments to the Consumer Protection Act[384] provides reasons to believe that in the near future more legislative acts will expressly provide for blocking and takedown. However, it is highly unlikely that these censoring techniques will be codified in a single piece of legislation as they govern a wide variety of issues of various nature. Moreover, the circumstances in virtual reality are extremely dynamic and preclude the legislative of regulating the matter exhaustively.

In conclusion, in the next five years the legislation regarding censoring of internet content and the liability of intermediaries will further develop. Executive agencies will be granted a wider margin of appreciation, while internet intermediaries will most likely have to abide by a higher standard. Moreover, it is expected that blocking and takedown will be explicitly addressed in the Bulgarian legal system more frequently. Nevertheless, these issues won't find their regulation within a single act.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

In order to analyse the issue of maintaining an adequate balance between ensuring freedom of expression online and protection against hate speech, firstly the term hate speech should be defined. Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination declares an offence punishable by law 'all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof.'[385] Hate speech is also to be

384 State Gazette No. 13, issued on 14 February 2020, pages 2-7.

385 *I*nternational Convention on the Elimination of All Forms of Racial Discrimination, Article 4 (a).

understood as 'covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.'[386] Hate speech as a social phenomenon illustrates the issue of finding the right balance between securing the right of freedom of expression (both offline and online) and the prevention of violation of other fundamental human rights, particularly regarding the dignity of the individual, a principle protected both in the Preamble and in Article 4 of the Constitution of The Republic of Bulgaria. Hate speech is also inextricably linked to the prohibition of discrimination on a different basis. In accordance with international agreements concerning the prohibition of discrimination, to which the Republic of Bulgaria is a State Party, in 2003 the Bulgarian Discrimination Protection Act is adopted.[387] This act banns 'any direct or indirect discrimination'[388] and includes various detailed legal measures for the protection against 'all forms of discrimination',[389] such as proceedings before the Commission for Protection against Discrimination, judicial proceedings, compulsory administrative measures, and administrative penal provisions.

Regarding the Bulgarian legislation, freedom of expression, on the other hand, is protected foremost on a constitutional level, in Article 39, Chapter 2, Fundamental Rights and Duties of the Citizens, of the Constitution of the Republic of Bulgaria. Nevertheless, subparagraph 2 states that this right shall not be used to the detriment of the rights and reputation of others, or for the incitement of a forcible change of the constitutionally established order, the perpetration of a crime, or the incitement of enmity or violence against anyone.[390] As the Bulgarian Constitutional Court states, the restriction regarding statements, which encourage hostility and hate, is based on the values, laid down in the Bulgarian Constitution, such as tolerance, mutual respect, as well as the prohibition of promoting hate based on race, nationality, ethnic origin or religion. This restriction does not exclude the protection of the diversity of contradictory opinions.[391] Hence, these are the established restrictions of the scope of freedom of expression on a national level. Moreover, the Case law of the European Court of Humans Rights should be taken into account on this matter, as the Republic of Bulgaria is a State Party to the European Convention

386 Appendix to Recommendation No. R (97)20 of the Committee of Ministers to member states on hate speech, page 107.
387 Drumeva, E., Constitutional Law, 2008.
388 Article 4 of the Protection against Discrimination Act 2004.
389 Article 1 of the Protection against Discrimination Act 2004.
390 Article 39 (2) of the Constitution of the Republic of Bulgaria 1991.
391 Simona Veleva, Freedom of Speech, Sofia University Press, 2020, page 275.

on Human Rights since 1992. The principle established in the case of *Handyside v. the United Kingdom* is 'that "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also those that offend, shock or disturb the State or any sector of the population' are covered by freedom of expression.[392] This principle should be considered when imposing any restrictions on freedom of speech, whether offline or online, and when determining whether it can be classified as hate speech, or not.

At the present moment, there are no explicit provisions in Bulgarian law governing internet censorship as a legal measure for preventing hate speech particularly online. There is the overall responsibility of liability for damages under Article 45 of the Bulgarian Law of Obligations and Contracts, which states that every person must redress the damage he has guiltily caused to another person and in all cases of tort guilt is presumed until proven otherwise. This article is applicable also when rights of persons are violated through speech. Hate inciting comments on internet sites, on the other hand, are mostly filtered or blocked by broadband, internet or email providers and search engines, as well as by the moderators of the particular website. In the latter case, the comments are removed, owing to the fact that they contravene the common rules of the website. Generally, these rules ban the spreading of hate inciting or discriminatory statements, although the procedure and criteria of removing content are not in all cases transparent, as there aren't established any clear legal limitations of the censorship on a national level. Consequently, the lack of legal guidelines, on the one hand, could lead to unnecessary and illegitimate blocking or filtering, which may threaten the freedom of expression online. On the other hand, some acts of hate speech could remain online, not being subjected to removal. Thus, it is of fundamental importance to maintain a balanced legal approach towards cases of hate speech online. In connection with hate speech offline, however, are to be found other legal measures in some articles of the Constitution of the Republic of Bulgaria, the Bulgarian Criminal Code and the Bulgarian Radio and Television Act.

According to the Second Principle of the Appendix to Recommendation No. R (97)20 of the Committee of Ministers to member states on hate speech, 'the governments of the member states should establish or maintain a sound legal framework consisting of civil, criminal and administrative law provisions on hate speech…'. Concerning the Bulgarian legislation, hate speech is criminalised and falls under the scope of Chapter 3, Crimes against the rights of the citizens, Section I, Crimes against the Equality of All Citizens of the Bulgarian Criminal

[392] Handyside v. the United Kingdom, 5493/72, ECtHR.

Code. According to Article 162 of the Bulgarian Criminal Code, anyone who, by speech, press or other media, by electronic information systems or in another manner, propagates or incites discrimination, violence or hatred on the grounds of race, nationality or ethnic origin shall be punishable by imprisonment from one to four years and a fine from BGN 5.000 to 10.000, as well as public censure.[393] This article should also apply to cases regarding hate speech online, considering the fact that the internet is a forum for free expression of unprecedented scope and importance.[394] It is one of the main means of distributing information, ideas and opinions on a daily basis globally, especially discriminatory and hate inciting statements, mainly due to the possibility for anonymity.

Another aspect of the Bulgarian law provisions regarding hate speech includes hate speech spread by the media service providers. Restrictions in Bulgaria related to the expression of discriminative opinions and verbal or written acts of harassment are regulated in terms of the media and press. According to Article 17 of the Bulgarian Radio and Television Act, 'Media service providers shall be obligated not to suffer the creation or provision for distribution of any programmes in violation of the principle of Article 10 herein, and any broadcasts inciting to national, political, ethnic, religious or racial intolerance, extolling or condoning brutality or violence […].'[395]

In conclusion, the principles established in the Bulgarian legislation for the punishment of hate speech events offline should be implemented regarding cases of online hate speech. At the same time, offline free expression protection guarantees also need to be applied to online situations, even if these have to be developed in recognizance of the special impact Internet publications often have.[396] It is stated in point one of the Preamble of Recommendation CM/Rec (2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries that 'Council of Europe member States have the obligation to secure the rights and freedoms enshrined in the Convention to everyone within their jurisdiction, both offline and online.' Furthermore, the international and European legislation on the matter should be adopted by the Bulgarian legislator, in order to achieve a comprehensive and clear legal framework concerning cases of hate speech. In addition, if any online content is considered as hate speech, it should be subjected to filtering or

393 Article 162 (1) of the Bulgarian Criminal Code 1968.

394 Nunziato, D., Virtual freedom. Net Neutrality and Free Speech in the Internet Age, 1st ed., Stanford, Stanford University Press 2009, page 1.

395 Radio and Television Act 1999, Article 17 (2).

396 Benedek, W., Kettemann, M. Freedom of expression and the internet, Council of Europe Publishing, 2013.

blocking, only while adhering to the three criteria for restriction; legality, legitimacy, and necessity, in order to avoid disproportionate banning of access to Internet content. Internet censorship should not be strictly regulated, as it is fundamental to maintain a balance between the prevention of spreading hate speech online and protecting the freedom of expression of the individuals.[397] This could be accomplished through a combination of all proposed solutions for regulations in this field – regulations by hard law and self-regulation through soft law; global regulation and national state regulation.[398]

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

The legal order is a system of norms.[399] As such, it establishes a logical coherency of its provisions in their relation to one another. The question of balance, therefore, is no more than the task of recognizing the scope of different legal norms in case of conflict. As for the term adequate, it can be taken in its general use of signifying that which is sufficient for a specific requirement[400] - in this case, the requirements of all constitutional and international obligations taken by the Bulgarian State that ensure the protection of human rights. Therefore, to answer whether an adequate balance between allowing freedom of expression online and protecting other rights has been reached in Bulgaria two questions need to be examined:

— The scope of the right to freedom of expression in the national legal system; and

— Whether the grounds for restricting the right to freedom of expression correspond to the international standards that Bulgaria has obliged itself to respect;

As it has been noted elsewhere, the right to freedom of expression online is encompassed in the provisions of Articles 39-41 of the Bulgarian Constitution and is not subject to a specific legal framework. Rather, its scope falls within the

397 Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom.

398 Nachev, D. Challenges to the Rule of Law at the Beginning of the Twenty-First Century with Regard to Freedom of Expression and Freedom of Information.

399 Kelsen, Hans. General Theory of Law and State (Harvard University Press 1949) page 110.

400 Merriam Webster, Adequate <https://www.merriam-webster.com/dictionary/adequate> accessed 20 February 2020.

same restrictions governing the other communication rights.[401] Enshrining the right to freedom of expression in the Bulgarian Constitution, the national legislator has sought to ensure its fundamental importance for the functioning of the adopted constitutional model of parliamentary democracy. As the only legitimate authority, empowered to interpret the Bulgarian Constitution,[402] the Constitutional Court of Bulgaria has regarded the question of balance between allowing freedom of expression and protecting other rights in its 1996 Decision № 7. Among others, the cited case defines the right to freedom of expression as well as an interpretation of its scope and is important, for these reasons, in the following regards.

Following the request of the Bulgarian President, the Constitutional Court issued an Advisory Opinion on the Provisions of Articles 39 - 41 of the Constitution. Assigned with the interpretation of the right to freedom of expression, the Court declared its fundamental character, while at the same time recognising its non-absolute scope. Reiterating its reluctance to declare a hierarchy of the principles and rights enshrined in the Constitution,[403] the Court, nonetheless, finds certain limits to the right in question, drawn out from the provisions of the Constitution itself. Beyond these constitutional grounds for restriction, however, the Court forbids the confinement of the right to freedom of expression.

In its systematic approach to interpreting the scope of the right to freedom of expression, the Constitutional Court of Bulgaria classifies the following categories of interests that can give ground to the restriction of communication rights:

— protection of the constitutional model adopted by Bulgaria (Article 39(2).; Article 40(2).);

— protection of national security (Article 41(1));

— protection of the public order and prevention of crime (Article 39(2); Article 40(2).; Article 41);

— protection of public health (Article 40(2).; Article 41(1));

— protection of the dignity and rights of other individuals (Article 39(2); Article 40(2).; Article 41(1), (2));

— protection of the right to privacy (Article 41(2)).

401 Simona Veleva, Freedom of Speech, Sofia University Press, 2020, page 300.
402 Article 149.1.1 of the Constitution of the Republic of Bulgaria 1991.
403 Decision №7/1996 of Constitutional Court of Bulgaria.

The classification, the Court notes, is conditional and it serves the purpose of answering the question whether a hierarchy among these restrictions can be established so that certain interests are given a higher priority than others. While considering it inappropriate to set predefined guidelines rather than allowing the judiciary bodies in the country to work out their case-specific solutions, the Court, nevertheless, acknowledges that the Constitution of Bulgaria gives special priority to the rights of the individual and, for this reasons, affirms that the possibility to restrict the right to freedom of expression to protect the right to dignity or other individual rights is higher.

Further down its decision, the Court also explores the relationship that the right to freedom of expression has to the public political order. Understanding it as a right defending the individual from the latter, the Constitutional Court of Bulgaria proclaims the negative obligation of the State not to interfere in the freedom of expression of the private citizen beyond the restrictively defined limits.

The aforementioned Decision of the Bulgarian Constitutional Court regards the issue of the scope of a fundamental human right, revealing carefully thought out limits to the freedom of expression. To conclude whether the balance achieved in the national legal system is adequate, meaning - in concord with international standards - it needs to be examined whether the constitutional grounds for restriction of this right deviate from international practice and breach the obligations taken by the Bulgarian State in this field.

When drafting the Constitution of Bulgaria, the working committee took into account all relative international legal documents that ensure the protection of human rights. Seeking to build a democratic society in a post-totalitarian reality, the legislator embedded internationally acknowledged principles into the Constitution of Bulgaria, found in legal documents such as the International Covenant on Civil and Political Rights, and the European Convention on Human Rights. Thus, Article 10. 2 of the latter contains the same grounds for restricting the right to freedom of expression as in the Bulgarian Constitution.

Beyond that, Bulgaria's membership in the EU as well as its readiness to comply with Union Law further ensure the alignment of national practice with international standards and recommendations.

For these reasons, the right to freedom of expression online, although lacking specific regulation, steps on an established body of practice - both national and international - that ensure its application within clearly defined limits that respect and correspond to the legal requirements of a democratic society.

10. How do you rank the access to freedom of expression online in your country?

Bulgaria's legal system regarding Internet censorship has its positive and negative sides. As a member state of the European Convention on Human Rights, a member of the European Union and an active member of the United Nations, Bulgaria has accepted human rights as a fundamental part of its legal system and has presented them in The Constitution of The Republic of Bulgaria. Bulgaria's legislative system implements international practices regarding the defence of human rights and the regulation of Internet activity. The country meets the problem of the new kind of relations the global web creates. Human rights must be regulated by censorship to the extent that it creates a safe environment for users but not at the cost of their freedom. Following the development of Internet activity, the state has improved its legislature so it may meet the needs of modern society. What must be mentioned is that common crimes, which can also be committed online, have been regulated. Also, the legal system provides a wide variety of safeguards against human rights offenses: numerous commissions that can take administrative measures, court trials against perpetrators and civil compensations for the victims. Regardless of the width of the acts, the State also creates the legal obligation for moderators of ISPs to block, take down or filter inappropriate content and assist authorities when there is a crime related to data of their user. However, there is no universal mechanism that can take down, filter or block illegal content. Also, The Swiss Institute of Comparative Law finds the lack of specific regulations concerning press and electronic media problematic. A lot of regulations concerning different sectors are based on the so-called 'soft law' which consists mainly of ethical codes. Regarding censorship on the Internet, as said before, a huge part plays the self-regulation of content that is in the hands of moderators. This provides a wide range of freedom of expression, but it also creates the possibility that illegal content is not taken down. Websites, social media, and forums have their own terms and conditions but there is no legal framework that establishes clear legal limitations of censorship on a national level. This threatens freedom of expression because it does not guarantee transparent criteria for removing content. Another problem that Bulgaria's legislative system faces is that due to the new field online environment presents, there is little to none legal practice and most of the sanctions and rules regarding it were originally created for the physical world.

In conclusion, we would rate Bulgarian Internet censorship as 5 out of 5 where 5 is the freedom of expression. While there are a lot of articles scattered around different acts that regulate digital reality, there is no clear framework for

censorship criteria. However, we must mention that the state holds accountable ISPs for illegal content that they or via their services is published. We should also accredit the different measures for securing human rights online that the legislative system provides. Also, we can notice that with the development of web relations, the Bulgarian law system evolves and tries to implement new regulations that meet the newly created needs.

11. How do you overall assess the legal situation in your country regarding internet censorship?

The present report concludes that the online environment offers a contemporary manifestation of the communication rights and therefore freedom of expression online falls within the general scope of Articles 39-41 of the Bulgarian Constitution.

The Constitution of Bulgaria prohibits censorship in all its forms. However, the constitutional grounds for exception of this prohibitive rule were mentioned in part 9 of the report. In line with them, separate national and international legal acts address cases where online content can be taken down or a website blocked.

In its 1996 Decision №7, previously discussed in line with the question of balancing constitutional rights, the Bulgarian Constitutional Court discussed the prohibition of censorship, defining the latter as any form of interference in the freedom of the press, specifically underlining the importance of protecting this right against State interference.

In practice, this general legal framework has provided sufficient assurance that the prohibition of censorship will remain in force in the online environment, despite the challenges and risks it poses.

Despite the scarcity of cases where this issue has been invoked, a conclusion can be drawn that the judiciary bodies of Bulgaria are compliant with the Constitutional requirements and the international obligations of the State and have worked to secure a safe internet environment. In fact, a study published on Comparitech ranks Bulgaria's online access, alongside that of States such as Belgium, Germany, France and Poland, among the world's most equal and open ones.[404]

[404] Comparitech, Internet Censorship 2020: A Global Map of Internet Restrictions <https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/> accessed 25 February 2020.

Conclusion

The right to freedom of expression online in Bulgaria does not have its specific regulation. Instead, it enjoys the same scope that the other communication rights, encompassed in the Constitution of the Republic of Bulgaria, have; or else, the national legal system regulates only certain aspects of its manifestation (for example in the field of cybersecurity).

Although the national legislator avoids drafting a legal framework, Bulgaria remains constant in its compliance with EU Law and EU policies, adopting its national legislation to the Union standards. Numerous studies, in fact, conclude that the national judiciary bodies express an ever-growing tendency to apply European Law more often than they do the Constitution itself, understanding the legal system of the Union as an inseparable and vital part of their activity.

The benefit of this approach is the guaranteed alignment of Bulgarian law with international practices and the readiness to cooperate on a supranational level and adopt unifying standards that better correspond to the transboundary nature of the internet environment.

The technological revolution, initiated in the past century, continues to stride in a pace, difficult for the legal order to keep up to at all times. Given their conservative nature and aim to set lasting rules governing a body of generic patterns of human behaviour, it is understandable why different legal systems would choose to leave certain areas of a society governed by broader legal norms, needing more time to properly analyse and crystallise a set of rules that can be adapted.

In conclusion, the nature of the internet is global and dynamic. This predisposes supranational cooperation in the field of internet censorship and freedom of expression online to establish a unified legal framework, rather than allowing separate actors to look for isolated solutions. In this sense, the approach of the national legislator is perhaps more preferable than rushing to codify, although, for the present, it does leave significant areas of internet activities under regulated and prone to violations and risks.

Table of legislation

Provision in Bulgarian language	**Corresponding translation in English**
Закон за радиото и телевизията Чл. 1. (Изм. - ДВ, бр. 12 от 2010 г.) Този закон урежда медийните услуги, предоставяни от доставчици на медийни услуги под юрисдикцията на Република България.	Radio and Television Act Article 1. (Amended, SG No. 12/2010) This Act shall regulate the media services provided under the jurisdiction of the Republic of Bulgaria.
Закон за радиото и телевизията Чл. 2. (Изм. - ДВ, бр. 12 от 2010 г.) (1) Медийни услуги по смисъла на този закон са аудио-визуални медийни услуги и радиоуслуги. (2) Аудио-визуална медийна услуга/радиоуслуга е: 1. услуга, така както е определена в чл. 56 и 57 от Договора за функционирането на Европейския съюз (ОВ, С 115/47 от 9 май 2008 г.), която е в рамките на редакционната отговорност на доставчик на медийни услуги, чиято основна цел е предоставянето на аудио-визуални предавания/радиопредавания за информиране, забавление или образоване на широката общественост чрез електронни съобщителни мрежи по смисъла на Закона за електронните съобщения; 2. аудио-визуално търговско съобщение/търговско съобщение в радиоуслуга по т. 1. (3) Аудио-визуално предаване е поредица от движещи се изображения със или без звук, което представлява обособена част от програмна схема или каталог, утвърден от доставчик на аудио-визуални медийни услуги и чиято форма е сравнима с формата и съдържанието на телевизионно излъчване. (4) Радиопредаване е обособена част от програмна схема на радиопрограма или	Radio and Television Act Article 2. (Amended, SG No. 12/2010) (1) Within the meaning given by this Act, "media services" shall be audiovisual media services and radio services. (2) "Audiovisual media service/radio service" means: 1. a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union (OJ C 115/47 of 9 May 2008 which is under the editorial responsibility of a media service provider and the principal purpose of which is the provision of audiovisual programmes/radio programmes in order to inform, entertain or educate the general public by electronic communications networks within the meaning given by the Electronic Communications Act; 2. an audiovisual commercial communication/commercial communication in a radio service referred to in Item 1. (3) "Audiovisual programme" means a set of moving images with or without sound constituting an individual item within a programme schedule or a catalogue established by a media service provider and whose form is comparable to the form and content of television broadcasting. (4) "Radio programme" means an individual item within a programme schedule of a radio programme service or a catalogue established by a radio service provider. (5) The provisions of this Act shall not apply to: 1. media services which are not for mass communication, i.e. are not intended for a substantial proportion of the public; 2. activities which are primarily non-

каталог, утвърден от доставчик на радиоуслуги. (5) Разпоредбите на този закон не се прилагат за: 1. медийни услуги, които не са за масово осведомяване, т.е. не са предназначени за значителна част от аудиторията; 2. дейности, които по принцип са с нестопански характер и които не са конкурентни на телевизията въз основа на програмна схема; 3. лична кореспонденция на ограничен брой адресати чрез електронни съобщителни мрежи; 4. всички услуги, чиято основна цел не е предоставянето на предавания, т.е. когато аудио-визуалното съдържание е включено случайно в услугата и не е нейна основна цел; 5. игрите на късмета, в които се залагат пари, включително лотария, наддаване и други форми на хазарт, както и онлайн игри и програми за търсене, но не и предавания, изцяло посветени на хазартни игри или игри на късмета; 6. електронни варианти на вестници и списания; 7. самостоятелните текстови услуги.	economic and which are not in competition with television on the basis of a programme schedule; 3. private correspondence sent to a limited number of recipients over electronic communications networks; 4. all services whose principal purpose is not the provision of programmes, i.e. where any audiovisual content is merely incidental to the service and is not its principal purpose; 5. games of chance involving a stake representing a sum of money, including lotteries, betting and other forms of gambling services, as well as on-line games and search engines, but not broadcasts entirely devoted to gambling or games of chance; 6. electronic versions of newspapers and magazines; 7. stand-alone text-based services.
Закон за радиото и телевизията Чл. 4 (Изм. - ДВ, бр. 12 от 2010 г.) (1) Доставчик на медийни услуги е физическо лице - едноличен търговец, или юридическо лице, което носи редакционна отговорност за избора на съдържанието на медийната услуга и определя начина, по който тя е организирана. Редакционна отговорност е упражняването на ефективен контрол както върху избора на предавания, така и върху тяхната организация както в хронологичен ред при линейни услуги, така и в каталог при медийни услуги по заявка.	Radio and Television Act Article 4 (Amended, SG No. 12/2010) (1) "Media service provider" means a sole-trader natural person or a legal person who or which has editorial responsibility for the choice of the content of the media service and determines the manner in which the said service is organized. "Editorial responsibility" means the exercise of effective control both over the selection of the programmes and over their organization either in a chronological schedule, in the case of linear services, or in a catalogue, in the case of on-demand media services. (2) "Radio or television broadcaster" means a provider of

(2) Радио- или телевизионен оператор е доставчик на линейни медийни услуги (програми) за радио/телевизия въз основа на програмна схема. (3) Не са доставчици на медийни услуги лица, които само разпространяват програми, за които редакционна отговорност носят трети страни.	radio/television linear media services (programme services) on the basis of a programme schedule. (3) Persons who or which merely distribute programme services for which the editorial responsibility lies with third parties shall not be media service providers.
Закон за радиото и телевизията Чл. 5 (Доп. - ДВ, бр. 79 от 2000 г., доп. - ДВ, бр. 93 от 2005 г., изм. - ДВ, бр. 12 от 2010 г.) (1) Този закон гарантира независимост на доставчиците на медийни услуги и на тяхната дейност от политическа и икономическа намеса.	Radio and Television Act Article 5 (Supplemented, SG No. 79/2000, SG No. 93/2005, amended, SG No. 12/2010) (1) This Act guarantees the freedom of media service providers and of the activities thereof from political and economic interference.
Закон за радиото и телевизията Чл. 8 (Изм. - ДВ, бр. 96 от 2001 г., изм. - ДВ, бр. 77 от 2002 г., изм. - ДВ, бр. 12 от 2010 г.) (1) Медийните услуги не трябва да подбуждат към ненавист, основана на раса, пол, религия или националност.	Radio and Television Act Article 8 (Amended, SG No. 96/2001, supplemented, SG No. 77/2002, amended, SG No. 12/2010) (1) Media services must not incite to hatred based on race, sex, religion or nationality.
Закон за радиото и телевизията Чл. 9 (Изм. - ДВ, бр. 79 от 2000 г., изм. - ДВ, бр. 12 от 2010 г.) (1) Доставчиците на медийни услуги разпространяват програми и предавания само с предварително уредени авторски и сродни на тях права.	Radio and Television Act Article 9 (Amended, SG No. 79/2000, SG No. 12/2010) (1) Media service providers shall distribute programme services and programmes solely after the copyrights and neighbouring rights have been settled in advance.
Закон за радиото и телевизията Чл. 15. (1) (Изм. - ДВ, бр. 96 от 2001 г., изм. - ДВ, бр. 12 от 2010 г.) Доставчиците на медийни услуги не са длъжни да разкриват източниците на информация, освен ако има висящо съдебно производство или висящо производство по жалба на засегнато лице, на Съвета за електронни медии.	Radio and Television Act Article 15. (1) (Amended, SG No. 12/2010) Media service providers shall not be obligated to disclose their sources of information to the Council for Electronic Media, save in the case of pending legal proceedings or pending proceedings initiated on the complaint of a person affected. (2)

(2) (Изм. - ДВ, бр. 12 от 2010 г.) Журналистите не са длъжни да разкриват източниците на информация не само пред аудиторията, но и пред ръководството на доставчик на медийни услуги, освен в случаите по ал. 1. (3) (Изм. - ДВ, бр. 12 от 2010 г.) Доставчиците на медийни услуги имат право да включват в предавания информация от неизвестен източник, като изрично посочват това. (4) Журналистите са длъжни да пазят в тайна източника на информация, ако това изрично е поискано от лицето, което я е предоставило.	(Amended, SG No. 12/2010) Journalists shall not be obligated to disclose their sources of information either to the audience or to the management of a media service provider, save in the cases under Paragraph (1). (3) (Amended, SG No. 12/2010) Media service providers shall have the right to include information from an unidentified source in their programmes, expressly stating this fact. (4) Journalists shall be obligated to protect the confidentiality of the source of information should this have been expressly requested by the person who has provided the said information.
Закон за радиото и телевизията Чл. 17 (1) (Изм. - ДВ, бр. 12 от 2010 г.) Доставчиците на медийни услуги носят отговорност за съдържанието на медийните услуги. (2) (Изм. - ДВ, бр. 12 от 2010 г., изм. - ДВ, бр. 28 от 2011 г.) Доставчиците на медийни услуги са длъжни да не допускат създаване или предоставяне за разпространение на предавания в нарушение на принципите на чл. 10 и предавания, внушаващи национална, политическа, етническа, религиозна и расова нетърпимост, възхваляващи или оневиняващи жестокост или насилие, или на предавания, които са неблагоприятни или създават опасност от увреждане на физическото, психическото, нравственото и/или социалното развитие на децата, съгласно критериите по чл. 32, ал. 5.	Radio and Television Act Article 17 (1) (Amended, SG No. 12/2010) Media service providers shall be accountable for the content of the media services. (2) (Amended, SG No. 12/2010, SG No. 28/2011) Media service providers shall be obligated not to suffer the creation or provision for distribution of any programmes in violation of the principles of Article 10 herein, and any broadcasts inciting to national, political, ethnic, religious or racial intolerance, extolling or condoning brutality or violence, or any broadcasts which are adverse to, or pose a risk of impairing, the physical, mental, moral and/or social development of children, according to the criteria referred to in Article 32 (5) herein.
Закон за радиото и телевизията Чл. 20 (Изм. - ДВ, бр. 96 от 2001 г.) (1) (Изм. - ДВ, бр. 12 от 2010 г.) Съветът за	Radio and Television Act Article 20

електронни медии е независим специализиран орган, който регулира медийните услуги в случаите и по реда, предвидени в този закон. (2) (Изм. - ДВ, бр. 12 от 2010 г.) При осъществяване на своята дейност Съветът за електронни медии се ръководи от интересите на обществото, като защитава свободата и плурализма на словото и информацията и независимостта на доставчиците на медийни услуги.	(Amended, SG No. 96/2001) (1) (Amended, SG No. 12/2010) The Council for Electronic Media shall be an independent specialized body which regulates media services in the cases and according to the procedure provided for in this Act. (2) (Amended, SG No. 12/2010) In the performance of its activity, the Council for Electronic Media shall be guided by the public interest, protecting the freedom and pluralism of speech and information and the independence of media service providers.
Закон за авторското право и сродните му права Чл. 94щ (9) При установяване на нарушение на този дял от организация за колективно управление на права или независимо дружество за колективно управление на права министърът на културата или оправомощен от него заместник-министър издава задължително предписание и определя подходящ срок за изпълнението му. Предписанието се връчва на лицето и се публикува на интернет страницата на Министерството на културата в тридневен срок от издаването му.	Copyright and Neighbouring Rights Act Article 94sht (9) Upon establishment of a violation of this share by a collective management organization or an independent collective management company, the Minister of Culture or a deputy minister authorized by him shall issue a mandatory prescription and shall set an appropriate term for its implementation. The prescription is handed to the person and is published on the website of the Ministry of Culture within three days of its issuance.
Закон за авторското право и сродните му права Чл. 95 (Изм. - ДВ, бр. 99 от 2005 г., в сила от 10.01.2006 г., предишен чл. 94 - ДВ, бр. 28 от 2018 г., в сила от 29.03.2018 г.) (1) Който наруши авторско право, сродно на него право или друго право по този закон, дължи обезщетение на носителя на правото или на лицето, на което той е отстъпил изключително право за използване. (2) Обезщетение се дължи за всички вреди, които са пряка и непосредствена последица от нарушението. (3) При определяне размера на обезщетението съдът взема предвид и всички обстоятелства, свързани с	Copyright and Neighbouring Rights Act Article 95 (1) Whoever infringes a copyright, a related right or another right under this law, shall owe compensation to the holder of the right or to the person to whom he has assigned an exclusive right for use. (2) Compensation shall be due for all damages, which are a direct and immediate consequence of the violation. (3) In determining the amount of the compensation the court shall also take into account all circumstances related to the violation, the lost benefits and the non-pecuniary damages, as well as the incomes, realized by the infringer as a result of the violation.

нарушението, пропуснатите ползи и неимуществените вреди, както и приходите, реализирани от нарушителя вследствие на нарушението. (4) Съдът определя справедливо обезщетение, което трябва да въздейства възпиращо и предупредително на нарушителя и на останалите членове на обществото.	(4) The court shall determine a fair compensation, which shall have a deterrent and warning effect on the offender and on the other members of the society.
Закон за защита от дискриминацията Чл. 1 Този закон урежда защитата срещу всички форми на дискриминация и съдейства за нейното предотвратяване.	Protection Against Discrimination Act Article 1 This Act shall regulate the protection against all forms of discrimination and shall contribute to its prevention.
Закон за защита от дискриминацията Чл.4(1) (1) (Доп. - ДВ, бр. 70 от 2004 г., в сила от 01.01.2005 г.) Забранена е всяка пряка или непряка дискриминация, основана на пол, раса, народност, етническа принадлежност, човешки геном, гражданство, произход, религия или вяра, образование, убеждения, политическа принадлежност, лично или обществено положение, увреждане, възраст, сексуална ориентация, семейно положение, имуществено състояние или на всякакви други признаци, установени в закон или в международен договор, по който Република България е страна.	Protection Against Discrimination Act Article 4(1) (1) (Amended SG No. 70/2004 - effective 1.01.2005) Any direct or indirect discrimination on grounds of gender, race, nationality, ethnicity, human genome, citizenship, origin, religion or belief, education, convictions, political affiliation, personal or social status, disability, age, sexual orientation, marital status, property status, or on any other grounds established by law or by an international treaty to which the Republic of Bulgaria is a party, shall be banned.
Закон за защита от дискриминацията Чл.47(1) Комисията за защита от дискриминация: 1. установява нарушения на този или други закони, уреждащи равенство в третирането, извършителя на нарушението и засегнатото лице;	Protection Against Discrimination Act Article 47(1) The Commission for Protection against Discrimination shall: 1. ascertain violations of this or other Acts regulating equal treatment, the perpetrator of the violation and the aggrieved person;

Конституцията на Република България Чл.6 (1) Всички хора се раждат свободни и равни по достойнство и права. (2) Всички граждани са равни пред закона. Не се допускат никакви ограничения на правата или привилегии, основани на раса, народност, етническа принадлежност, пол, произход, религия, образование, убеждения, политическа принадлежност, лично и обществено положение или имуществено състояние.	Constitution of the Republic of Bulgaria Article 6 (1) All persons are born free and equal in dignity and rights. (2) All citizens* shall be equal before the law. There shall be no privileges or restriction of rights on the grounds of race, national or social origin, ethnic self-identity, sex, religion, education, opinion, political affiliation, personal or social status or property status.
Конституцията на Република България Чл.14 Семейството, майчинството и децата са под закрила на държавата и обществото.	Constitution of the Republic of Bulgaria Article 14 The family, motherhood and children shall enjoy the protection of the State and society.
Конституцията на Република България Чл.32 (1) Личният живот на гражданите е неприкосновен. Всеки има право на защита срещу незаконна намеса в личния и семейния му живот и срещу посегателство върху неговата чест, достойнство и добро име. (2) Никой не може да бъде следен, фотографиран, филмиран, записван или подлаган на други подобни действия без негово знание или въпреки неговото изрично несъгласие освен в предвидените от закона случаи.	Constitution of the Republic of Bulgaria Article 32 (1) The privacy of citizens shall be inviolable. Everyone shall be entitled to protection against any unlawful interference in his private or family affairs and against encroachments on his honour, dignity and reputation. (2) No one shall be followed, photographed, filmed, recorded or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law.
Конституцията на Република България Чл.34 (1) Свободата и тайната на кореспонденцията и на другите съобщения са неприкосновени. (2) Изключения от това правило се допускат само с разрешение на съдебната власт, когато това се налага за разкриване или предотвратяване на тежки престъпления.	Constitution of the Republic of Bulgaria Article 34 (1) The freedom and confidentiality of correspondence and all other communications shall be inviolable. (2) Exceptions to this provision shall be allowed only with the permission of the judicial authorities for the purpose of discovering or preventing a grave crime.
Конституцията на Република България Чл.39 (1) Всеки има право да изразява мнение и да го разпространява чрез слово -	Constitution of the Republic of Bulgaria Article 39 (1) Everyone shall be entitled to express an opinion or to publicize it through words,

писмено или устно, чрез звук, изображение или по друг начин. (2) Това право не може да се използва за накърняване на правата и доброто име на другиго и за призоваване към насилствена промяна на конституционно установения ред, към извършване на престъпления, към разпалване на вражда или към насилие над личността.	written or oral, sound or image, or in any other way. (2) This right shall not be used to the detriment of the rights and reputation of others, or for the incitement of a forcible change of the constitutionally established order, the perpetration of a crime, or the incitement of enmity or violence against anyone.
Конституцията на Република България Чл. 40 (1) Печатът и другите средства за масова информация са свободни и не подлежат на цензура. (2) Спирането и конфискацията на печатно издание или на друг носител на информация се допускат само въз основа на акт на съдебната власт, когато се накърняват добрите нрави или се съдържат призиви за насилствена промяна на конституционно установения ред, за извършване на престъпление или за насилие над личността. Ако в срок от 24 часа не последва конфискация, спирането преустановява действието си.	Constitution of the Republic of Bulgaria Article 40 (1) The press and the other mass information media shall be free and shall not be subjected to censorship. (2) An injunction on or a confiscation of printed matter or another information medium shall be allowed only through an act of the judicial authorities in the case of an encroachment on public decency or incitement of a forcible change of the constitutionally established order, the perpetration of a crime, or the incitement of violence against anyone. An injunction suspension shall lose force if not followed by a confiscation within 24 hours.
Конституцията на Република България Чл.41 (1) Всеки има право да търси, получава и разпространява информация. Осъществяването на това право не може да бъде насочено срещу правата и доброто име на другите граждани, както и срещу националната сигурност, обществения ред, народното здраве и морала. (2) Гражданите имат право на информация от държавен орган или учреждение по въпроси, които представляват за тях законен интерес, ако информацията не е държавна или друга защитена от закона тайна или не засяга чужди права.	Constitution of the Republic of Bulgaria Article 41 (1) Everyone shall be entitled to seek, obtain and disseminate information. This right shall not be exercised to the detriment of the rights and reputation of others, or to the detriment of national security, public order, public health and morality. (2) Everyone shall be entitled to obtain information from state bodies and agencies on any matter of legitimate interest to them which is not a state or official secret and does not affect the rights of others.
Конституцията на Република България Чл.54 (1) Всеки има право да се ползва от националните и общочовешките културни ценности, както и да развива	Constitution of the Republic of Bulgaria Article 54 (1) Everyone shall have the right to avail himself of the national and universal human

своята култура в съответствие с етническата си принадлежност, което се признава и гарантира от закона. (2) Свободата на художественото, научното и техническото творчество се признава и гарантира от закона. (3) Изобретателските, авторските и сродните на тях права се закрилят от закона.	cultural values and to develop his own culture in accordance with his ethnic self-identification, which shall be recognized and guaranteed by the law. (2) Artistic, scientific and technological creativity shall be recognized and guaranteed by the law. (3) The State shall protect all inventors' rights, copyrights and related rights.
Конституцията на Република България Чл.149 (1) Конституционният съд: 1. дава задължителни тълкувания на Конституцията ; 2. произнася се по искане за установяване на противоконституционност на законите и на другите актове на Народното събрание, както и на актовете на президента; 3. решава спорове за компетентност между Народното събрание, президента и Министерския съвет, както и между органите на местно самоуправление и централните изпълнителни органи; 4. произнася се за съответствието на сключените от Република България международни договори с Конституцията преди ратификацията им, както и за съответствие на законите с общопризнатите норми на международното право и с международните договори, по които България е страна; 5. произнася се по спорове за конституционността на политическите партии и сдружения; 6. произнася се по спорове за законността на избора за президент и вицепрезидент; 7. произнася се по спорове за законността на избора на народен представител; 8. произнася се по обвинения, повдигнати от Народното събрание срещу президента и вицепрезидента. (2) Със закон не могат да се дават или отнемат правомощия на Конституционния съд.	Constitution of the Republic of Bulgaria Article 149 (1) The Constitutional Court shall: 1. provide binding interpretations of the Constitution; 2. rule on constitutionality of the laws and other acts passed by the National Assembly and the acts of the President; 3. rule on competence suits between the National Assembly, the President and the Council of Ministers, and between the bodies of local self-government and the central executive branch of government; 4. rule on the compatibility between the Constitution and the international treaties concluded by the Republic of Bulgaria prior to their ratification, and on the compatibility of domestic laws with the universally recognized norms of international law and the international treaties to which Bulgaria is a party; 5. rule on challenges to the constitutionality of political parties and associations; 6. rule on challenges to the legality of the election of the President and Vice President; 7. rule on challenges to the legality of an election of a Member of the National Assembly; 8. rule on impeachments by the National Assembly against the President or the Vice President. (2) No authority of the Constitutional Court shall be vested or suspended by law.

Наказателен кодекс на Република България Чл. 78а (Нов - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г.) (1) (Изм. - ДВ, бр. 10 от 1993 г., изм. - ДВ, бр. 62 от 1997 г., изм. - ДВ, бр. 21 от 2000 г., изм. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006 г., изм. - ДВ, бр. 26 от 2010 г.) Пълнолетно лице се освобождава от наказателна отговорност от съда и му се налага наказание от хиляда до пет хиляди лева, когато са налице едновременно следните условия: а) (изм. - ДВ, бр. 86 от 2005 г., в сила от 29.04.2006 г.) за престъплението се предвижда наказание лишаване от свобода до три години или друго по-леко наказание, когато е умишлено, или лишаване от свобода до пет години или друго по-леко наказание, когато е непредпазливо; б) деецът не е осъждан за престъпление от общ характер и не е освобождаван от наказателна отговорност по реда на този раздел; в) причинените от престъплението имуществени вреди са възстановени. (2) (Отм. - ДВ, бр. 21 от 2000 г.) (3) (Отм. - ДВ, бр. 21 от 2000 г.) (4) Съдът, който налага глобата по ал. 1, може да наложи и административно наказание лишаване от право да се упражнява определена професия или дейност за срок до три години, ако лишаване от такова право е предвидено за съответното престъпление. (5) Когато за извършеното престъпление е предвидено само глоба или глоба и друго по-леко наказание, административното наказание не може да надвишава размера на тази глоба. (6) (Нова - ДВ, бр. 26 от 2010 г.) Когато са налице основанията по ал. 1 и деянието е извършено от непълнолетно лице, съдът го освобождава от наказателна	Criminal code of the Republic of Bulgaria Article 78a (New, SG No. 28/1982) (1) (Amended, SG No. 10/1993, SG No. 62/1997, SG No. 21/2000, SG No. 75/2006, SG No. 26/2010) A person of full legal age shall be released from penal responsibility by the court, whereas the punishment imposed on him shall be a fine from BGN 1,000 to BGN 5,000 where the following conditions are concurrently available: a) (amended, SG No. 86/2005) for such crime punishment by imprisonment for up to three years or another milder punishment is provided, if committed intentionally, or imprisonment for up to five years or another milder punishment, if committed through negligence; b) the perpetrator has not been sentenced for a common crime and has not been previously released from penal responsibility pursuant to this Section; and c) the damages to property, which have been caused by the crime, have been restored. (2) (Repealed, SG No. 21/2000). (3) (Repealed, SG No. 21/2000). (4) The court which imposes a fine under paragraph (1), may also impose administrative punishment by deprivation of the right to practice a certain vocation or activity for up to three years, if deprivation of such right has been provided for the respective crime. (5) Where for the crime committed a fine only, or a fine and another milder punishment have been provided, the administrative punishment may not exceed the amount of such fine. (6) (New, SG No. 26/2010) If the grounds under paragraph 1 are present and the act was committed by an underage person, the court shall exempt it from penal liability and shall impose on it an administrative punishment public censure or an educational measure. The court may also impose an administrative punishment deprivation of the right to exercise a certain vocation or activity for a period of up to

отговорност, като му налага административно наказание обществено порицание или възпитателна мярка. Съдът може да наложи и административно наказание лишаване от право да се упражнява определена професия или дейност за срок до три години, ако лишаване от такова право е предвидено за съответното престъпление. (7) (Нова - ДВ, бр. 86 от 2005 г., в сила от 29.04.2006 г., изм. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006 г., доп. - ДВ, бр. 27 от 2009 г., предишна ал. 6 - ДВ, бр. 26 от 2010 г., изм. - ДВ, бр. 95 от 2016 г., доп. - ДВ, бр. 54 от 2017 г.) Алинеи 1 - 6 не се прилагат, ако причиненото увреждане е тежка телесна повреда или смърт, или деецът е бил в пияно състояние, или след употреба на наркотични вещества или техни аналози, както и при множество престъпления както и когато престъплението е извършено спрямо орган на власт при или по повод изпълнение на службата му.	three years, if deprivation of such a right is foreseen for the respective crime. (7) (New, SG No. 86/2005, amended, SG No. 75/2006, supplemented, SG No. 27/2009, renumbered from Paragraph 6, SG No. 26/2010, amended, SG No. 95/2016, supplemented, SG No. 54/2017) Paragraphs 1 - 6 shall not apply where a severe bodily injury or death were inflicted, where the perpetrator had been in a state of drunkenness or after use of narcotic drugs or their analogues, as well as in the presence of a multitude of crimes and where the crime was committed against a government body of power during or in connection with the performance of his duty.
Наказателен кодекс на Република България Чл. 146 (1) (Изм. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. - ДВ, бр. 10 от 1993 г., изм. - ДВ, бр. 21 от 2000 г.) Който каже или извърши нещо унизително за честта или достойнството на другиго в негово присъствие, се наказва за обида с глоба от хиляда до три хиляди лева. В този случай съдът може да наложи и наказание обществено порицание. (2) Ако обиденият е отвърнал веднага с обида, съдът може да освободи и двамата от наказание.	Criminal code of the Republic of Bulgaria Article 146 (1) (Amended, SG No. 28/1982, SG No. 10/1993, SG No. 21/2000) A person who says or does something degrading to the honour and dignity of another in the presence of the latter, shall be punished for insult by a fine from BGN one thousand up to three thousand. In such a case the court may also impose the punishment of public censure. (2) If the insulted person has responded at once with an insult, the court may exempt both of them from punishment.
Наказателен кодекс на Република България Чл. 147	Criminal code of the Republic of Bulgaria Article 147 (1) (Amended, SG No. 28/1982, SG No. 10/1993, SG No. 21/2000) A person who

(1) (Изм. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. - ДВ, бр. 10 от 1993 г., изм. - ДВ, бр. 21 от 2000 г.) Който разгласи позорно обстоятелство за другиго или му припише престъпление, се наказва за клевета с глоба от три хиляди до седем хиляди лева и с обществено порицание. (2) Деецът не се наказва, ако се докаже истинността на разгласените обстоятелства или на приписаните престъпления.	makes public a disgraceful fact about someone or ascribes to him a crime, shall be punished for slander by a fine from BGN three thousand up to seven thousand, as well as by public censure. (2) The perpetrator shall not be punished if the truth of the divulged circumstances or of the ascribed crimes is proved.
Наказателен кодекс на Република България Чл. 148 (1) (Изм. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г.) За обида: 1. нанесена публично; 2. разпространена чрез печатно произведение или по друг начин; 3. на длъжностно лице или на представител на обществеността при или по повод изпълнение на службата или функцията му и 4. (изм. - ДВ, бр. 10 от 1993 г.) от длъжностно лице или от представител на обществеността при или по повод изпълнение на службата или функцията му, (изм. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г.) наказанието е глоба от три хиляди до десет хиляди лева и обществено порицание. (2) (Изм. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. - ДВ, бр. 21 от 2000 г.) За клевета, извършена при условията на предходната алинея, както и за клевета, от която са настъпили тежки последици, наказанието е глоба от пет хиляди лева до петнадесет хиляди лева и обществено порицание. (3) В случаите на ал. 1, точка 1 може да намери приложение ал. 2 на чл. 146.	Criminal code of the Republic of Bulgaria Article 148 (1) (Amended, SG No. 28/1982, SG No. 10/1993, SG No. 21/2000) For insult: 1. inflicted publicly; 2. spread through printed matter or in some other way; 3. of an official or a representative of the public, during or in connection with the fulfilment of his duties or function, and 4. by an official or representative of the public, during or in connection with the fulfilment of his duties or function, the punishment shall be a fine from BGN three thousand up to ten thousand as well as public censure. (2) (Amended, SG No. 28/1982, SG No. 21/2000) For slander committed under the conditions of the preceding paragraph, as well as for slander from which serious consequences have set in, the punishment shall be a fine from BGN five thousand up to fifteen thousand and public censure. (3) Paragraph (2) of Article 146 may be applied to cases under paragraph (1), sub-paragraph 1. Article 148a

Наказателен кодекс на Република България Чл. 159 (Изм. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. - ДВ, бр. 10 от 1993 г., изм. - ДВ, бр. 62 от 1997 г., изм. - ДВ, бр. 92 от 2002 г.) (1) (Изм. - ДВ, бр. 38 от 2007 г.) Който създава, излага, представя, излъчва, предлага, продава, дава под наем или по друг начин разпространява порнографски материал, се наказва с лишаване от свобода до една година и глоба от хиляда до три хиляди лева. (2) (Нова - ДВ, бр. 38 от 2007 г., доп. - ДВ, бр. 27 от 2009 г., изм. - ДВ, бр. 74 от 2015 г.) Който разпространява чрез информационна или съобщителна технология или по друг подобен начин порнографски материал, се наказва с лишаване от свобода до две години и глоба от хиляда до три хиляди лева. (3) (Предишна ал. 2, изм. - ДВ, бр. 38 от 2007 г.) Който излага, представя, предлага, продава, дава под наем или по друг начин разпространява порнографски материал на лице, ненавършило 16 години, се наказва с лишаване от свобода до три години и глоба до пет хиляди лева. (4) (Изм. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006 г., предишна ал. 3, изм. - ДВ, бр. 38 от 2007 г., изм. - ДВ, бр. 74 от 2015 г.) За деянието по ал. 1 - 3 наказанието е лишаване от свобода до шест години и глоба до осем хиляди лева, когато: 1. за създаването на порнографския материал е използвано лице, ненавършило 18-годишна възраст, или лице, което изглежда като такова; 2. за създаването на порнографския материал е използвано лице, което не разбира свойството или значението на извършеното; 3. е извършено от две или повече лица; 4. е извършено повторно.	Criminal code of the Republic of Bulgaria Article 159 (Amended, SG No. 28/1982, SG No. 10/1993, SG No. 62/1997, SG No. 92/2002) (1) (Amended, SG No. 38/2007) A person who produces, displays, presents, broadcasts, distributes, sells, rents or otherwise circulates a pornographic material, shall be punished by imprisonment of up to one year and a fine from BGN 1,000 to 3,000. (2) (New, SG No. 38/2007, supplemented, SG No. 27/2009, amended, SG No. 74/2015) Anyone who distributes pornographic material by means of information or communication technology or in another similar manner shall be punished by imprisonment for up to two years and a fine from BGN 1,000 to 3,000. (3) (Renumbered from paragraph 2 and amended, SG No. 38/2007) An individual who displays, presents, offers, sells, rents or distributes in another manner a pornographic material to a person who has not turned 16 years of age, shall be punished by imprisonment of up to three years and a fine of up to BGN 5,000. (4) (Amended, SG No. 75/2006, renumbered from Paragraph 3, amended, SG No. 38/2007, SG No. 74/2015) For acts under Paragraphs 1 - 3, the punishment shall be imprisonment for up to six years and a fine of up to BGN 8,000, where: 1. a person who has not reached 18 years of age (or anyone who looks like such a person) has been used for the production of the pornographic material; 2. a person who does not understand the nature or meaning of the act has been used for the creation of the pornographic material; 3. the act has been committed by two or more persons; 4. the act has been committed repeatedly. (5) (Renumbered from paragraph 4 and amended, SG No. 38/2007) Where acts under paras. 1 - 4 have been committed at the orders or in implementing a decision of an organized criminal group, punishment

(5) (Предишна ал. 4, изм. - ДВ, бр. 38 от 2007 г.) Когато деянието по ал. 1 - 4 е извършено по поръчение или в изпълнение на решение на организирана престъпна група, наказанието е лишаване от свобода от две до осем години и глоба до десет хиляди лева, като съдът може да постанови и конфискация на част или на цялото имущество на дееца. (6) (Предишна ал. 5, изм. - ДВ, бр. 38 от 2007 г., изм. - ДВ, бр. 74 от 2015 г.) Който държи или набавя за себе си или за другиго чрез информационна или съобщителна технология или по друг начин порнографски материал, за създаването на който е използвано лице, ненавършило 18 години, или лице, което изглежда като такова, се наказва с лишаване от свобода до една година и с глоба до две хиляди лева. (7) (Нова - ДВ, бр. 74 от 2015 г.) Наказанието по ал. 6 се налага и на онзи, който чрез информационна или съобщителна технология съзнателно осъществи достъп до порнографски материал, за създаването на който е използвано лице, ненавършило 18-годишна възраст, или лице, което изглежда като такова. (8) (Нова - ДВ, бр. 74 от 2015 г.) В случаите по ал. 1 - 7 съдът може да наложи и лишаване от право по чл. 37, ал. 1, т. 6 или 7. (9) (Предишна ал. 6 - ДВ, бр. 38 от 2007 г., предишна ал. 7 - ДВ, бр. 74 от 2015 г.) Предметът на престъплението се отнема в полза на държавата, а ако липсва или е отчужден, се присъжда неговата равностойност.	shall be imprisonment from two to eight years and a fine of up to BGN ten thousand (10,000), the court being also competent to impose confiscation of some or all the possessions of the perpetrator. (6) (Renumbered from paragraph 5 and amended, SG No. 38/2007, SG No. 74/2015) Anyone who, by means of information or communication technology or otherwise, possesses or provides for himself/herself or to another person pornographic material for the production of which a person under 18 years of age (or anyone who looks like such a person) has been used shall be punished by imprisonment of up to one year or a fine of up to BGN 2,000. (7) (New, SG No. 74/2015) The punishment under Paragraph 6 shall also be imposed on anyone who, by means of information or communication technology, has intentionally accessed pornographic material, for the production of which a person under 18 years of age (or anyone who looks like such a person) has been used. (8) (New, SG No. 74/2015) In the cases under Paragraphs 1 - 7, the court may also impose a punishment which entails deprivation of rights under Article 37, Paragraph 1, sub-paragraphs 6 or 7. (9) (Renumbered from Paragraph 6, SG No. 38 of 2007, renumbered from Paragraph 7, SG No. 74/2015) The object of criminal activity shall be confiscated to the benefit of the State, and where it is not found or has been expropriated, its money equivalent shall be awarded.
Наказателен кодекс на Република България Чл. 162 (1) (Изм. - ДВ, бр. 27 от 2009 г., изм. - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Който чрез слово, печат или други средства за масова информация, чрез	Criminal code of the Republic of Bulgaria Article 162 (1) (Amended, SG No. 27/2009, SG No. 33/2011, effective 27.05.2011) Anyone who, by speech, press or other media, by electronic information systems or in another manner, propagates or incites

електронни информационни системи или по друг начин проповядва или подбужда към дискриминация, насилие или омраза, основани на раса, народност или етническа принадлежност, се наказва с лишаване от свобода от една до четири години и с глоба от пет хиляди до десет хиляди лева, както и с обществено порицание. (2) (Изм. - ДВ, бр. 27 от 2009 г., изм. - ДВ, бр. 33 от 2011 г., в сила от 27.05.2011 г.) Който употреби насилие срещу другиго или повреди имота му поради неговата раса, народност, етническа принадлежност, религия или политически убеждения, се наказва с лишаване от свобода от една до четири години и с глоба от пет хиляди до десет хиляди лева, както и с обществено порицание. (3) (Изм. - ДВ, бр. 27 от 2009 г.) Който образува или ръководи организация или група, която си поставя за цел извършването на деяния по ал. 1 и 2 или системно допуска извършването на такива деяния, се наказва с лишаване от свобода от една до шест години и с глоба от десет хиляди до тридесет хиляди лева, както и с обществено порицание. (4) Който членува в такава организация или група, се наказва с лишаване от свобода до три години и с обществено порицание. (5) (Нова - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. - ДВ, бр. 92 от 2002 г., в сила от 01.01.2005 г., изм. относно влизането в сила - ДВ, бр. 26 от 2004 г., в сила от 01.01.2004 г., отм. - ДВ, бр. 103 от 2004 г., в сила от 01.01.2005 г.)	discrimination, violence or hatred on the grounds of race, nationality or ethnic origin shall be punishable by imprisonment from one to four years and a fine from BGN 5,000 to 10,000, as well as public censure. (2) (Amended, SG No. 27/2009, SG No. 33/2011, effective 27.05.2011) Anyone who uses violence against another person or damages his/her property because of the personTs race, nationality, ethnic origin, religion or political convictions, shall be punishable by imprisonment from one to four years and a fine from BGN 5,000 to 10,000, as well as public censure. (3) (Amended, SG No. 27/2009) A person who forms or leads an organisation or group which has set itself the objective of committing acts under paragraphs (1) and (2) or systematically allows the performance of such acts, shall be punished by imprisonment for one to six years and a fine from BGN ten thousand to thirty thousand and by public censure. (4) A person who is a member of such an organisation or group shall be punished by imprisonment for up to three years and by public censure. (5) (New, SG No. 28/1982, amended, SG No. 92/2002, effective 1.01.2005 with respect to the punishment
Наказателен кодекс на Република България Чл. 166 (Доп. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. - ДВ, бр. 92 от 2002 г., в сила от 01.01.2005 г., изм. относно влизането в сила - ДВ, бр. 26 от 2004 г., в	Criminal code of the Republic of Bulgaria Article 166 (Supplemented, SG No. 28/1982, amended, SG No. 92/2002, effective 1.01.2005 with respect to the punishment of probation - amended, SG No. 26/2004, effective 1.01.2004, SG No. 103/2004, SG No.

сила от 01.01.2004 г., изм. - ДВ, бр. 103 от 2004 г., в сила от 01.01.2005 г., изм. - ДВ, бр. 27 от 2009 г.) Който образува политическа организация на религиозна основа или който чрез слово, печат, действие или по друг начин използува църквата или религията за пропаганда против държавната власт или нейните мероприятия, се наказва с лишаване от свобода до три години, ако не подлежи на по-тежко наказание.	27/2009) A person who forms a political organisation on religious basis or who by speech, through the press, action or in another way, uses the church or religion for propaganda against the rule of the people or its undertakings, shall be punished by imprisonment for up to three years, if he is not subject to more severe punishment.
Наказателен кодекс на Република България Чл. 171 (1) (Изм. - ДВ, бр. 28 от 1982 г., в сила от 01.07.1982 г., изм. - ДВ, бр. 10 от 1993 г.) Който противозаконно: 1. отвори, подправи, скрие или унищожи чуждо писмо, телеграма, запечатани книжа пакет или други подобни; 2. (изм. - ДВ, бр. 92 от 2002 г.) вземе чуждо, макар и отворено писмо или телеграма с цел да узнае тяхното съдържание или пък със същата цел предаде другиму чуждо писмо или телеграма; 3. (нова - ДВ, бр. 92 от 2002 г.) узнае неадресирано до него съобщение, изпратено по електронен път, или отклони от адресата му такова съобщение, се наказва с лишаване от свобода до една година или с глоба от сто до триста лева (2) (Изм. - ДВ, бр. 75 от 2006 г., в сила от 13.10.2006 г.) Ако деянието е извършено от длъжностно лице, което се е възползувало от служебното си положение, наказанието е лишаване от свобода до две години, като съдът може да постанови и лишаване от право по чл. 37, ал. 1, точка 6. (3) (Доп. - ДВ, бр. 92 от 2002 г., доп. - ДВ, бр. 101 от 2017 г.) Който чрез използуване на специални технически средства противозаконно осъществи достъп до или узнае неадресирано до него съобщение, предадено по телефон,	Criminal code of the Republic of Bulgaria Article 171 (1) (Amended, SG No. 28/1982, SG No. 10/1993) A person who contrary to the law: 1. opens, falsifies, hides or destroys a letter, telegram, sealed papers, package and the like of another person; 2. takes another person's, although opened, letter or telegram for the purpose of obtaining knowledge of their contents, or for the same purpose delivers another person's letter or telegram to someone else; 3. (new, SG No. 92/2002) becomes aware of the content of an electronic message not addressed to him/her or prevents such a message from reaching its original addressee, shall be punished by imprisonment for up to one year or by a fine from BGN one hundred to three hundred. (2) If the act was perpetrated by an official who availed himself of his official position, the punishment shall by imprisonment for up to two years, and the court may also rule deprivation of the right under Article 37 (1), sub-paragraph 6. (3) (Supplemented, SG No. 92/2002) A person who, by use of special technical means, unlawfully obtains information not addressed to him, communicated over the telephone, telegraph, computer network or another telecommunication means, shall be punished by imprisonment for up to two years. (4) (New, SG No. 38/2007) Where the act under paragraph 3 has been committed with a venal goal in mind or considerable damages have been caused, the punishment shall be imprisonment for up to three years and a fine of up to BGN 5,000.

телеграф, чрез компютърна мрежа или по друго далекосъобщително средство, се наказва с лишаване от свобода до две години. (4) (Нова - ДВ, бр. 101 от 2017 г.) Наказанието по ал. 3 се налага и когато предмет на деянието са компютърни данни, изпращани в рамките на една или между повече информационни системи, включително електромагнитни емисии от информационна система. (5) (Нова - ДВ, бр. 38 от 2007 г., предишна ал. 4, доп. - ДВ, бр. 101 от 2017 г.) Когато деянието по ал. 3 и 4 е извършено с користна цел или са причинени значителни вреди, наказанието е лишаване от свобода до три години и глоба до пет хиляди лева.	
Наказателен кодекс на Република България Чл. 171а (Нов - ДВ, бр. 26 от 2010 г.) (1) (Изм. и доп. - ДВ, бр. 24 от 2015 г., в сила от 31.03.2015 г.) Който противозаконно придобие, съхранява, разкрие или разпространи данни, каквито се събират, обработват, съхраняват или използват съгласно Закона за електронните съобщения, се наказва с лишаване от свобода до три години или пробация. (2) Когато деянието по ал. 1 е извършено с користна цел, наказанието е лишаване от свобода от една до шест години.	Criminal code of the Republic of Bulgaria Article 171a (New, SG No. 26/2010) (1) (Amended and supplemented, SG No. 24/2015, effective 31.03.2015) A person who unlawfully acquires, stores, discloses or disseminates data as those collected, processed, kept or used as per the Electronic Communications Act, shall be punished by imprisonment up to three years or probation. (2) If the act under paragraph 1 was committed for a venal goal, the punishment shall be imprisonment from one to six years.
Наказателен-процесуален кодекс на Република България Чл. 159 (1) (Предишен текст на чл. 159 - ДВ, бр. 32 от 2010 г., в сила от 28.05.2010 г., изм. - ДВ, бр. 24 от 2015 г., в сила от 31.03.2015 г.) По искане на съда или на органите на досъдебното производство всички учреждения, юридически лица, длъжностни лица и граждани са длъжни	Criminal Procedure Code of Republic of Bulgaria Article 159 (1)(prev. text of Article 159 - SG 32/10, in force from 28.05.2010) On a request of the Court or of the bodies of the pre-trial procedures, all establishments, juridical persons, officials and citizens shall be obliged to preserve and deliver the objects, papers, computer information data, the

да запазят и предадат намиращите се у тях предмети, книжа, компютърни информационни данни и други данни, които могат да имат значение за делото. (2) (Нова - ДВ, бр. 32 от 2010 г., в сила от 28.05.2010 г.) Органите на досъдебното производство или съдът могат да поискат от директора на Европейската служба за борба с измамите да им предостави докладите и приложените към тях документи относно провеждани разследвания на службата.	carriers of such data and data about the subscriber, which are in their possession and may be of importance for the case. (2) (new –SG 32/10, in force from 28.05.2010) The pre-trial authorities or the Court may request from the European Anti-Fraud Office to provide the reports and the documents attached thereto regarding investigations conducted by the Office.
Закон за защита на личните данни Чл. 1 (4) Този закон урежда и: 1. статута на Комисията за защита на личните данни като надзорен орган, отговорен за защита на основните права и свободи на физическите лица във връзка с обработването и улесняването на свободното движение на лични данни в Европейския съюз; 2. правомощията на Инспектората към Висшия съдебен съвет при осъществяването на надзор при обработването на лични данни в случаите по чл. 17; 3. средствата за правна защита; 4. акредитирането и сертифицирането в областта на защитата на личните данни; 5. особени случаи на обработване на лични данни.	Personal Data Protection Act Article 1 (4) This Act furthermore governs: 1. the status of the Commission for Personal Data Protection as a supervisory authority responsible for the protection of the fundamental rights and freedoms of natural persons with regard to processing and facilitation of the free flow of personal data within the European Union; 2. the powers of the Inspectorate of the Supreme Judicial Council in the exercise of supervision regarding the processing of personal data in the cases referred to in Article 17; 3. the remedies; 4. accreditation and certification in the field of personal data protection; 5. specific data processing cases.
Закон за защита на личните данни Чл. 25а (Нов - ДВ, бр. 17 от 2019 г.) Когато лични данни са предоставени от субекта на данни на администратор или обработващ лични данни без правно основание по чл. 6, параграф 1 от Регламент (ЕС) 2016/679 или в	Personal Data Protection Act Article 25a (New, SG No 17 of 2019) Where any personal data has been provided by the data subject to a data controller or processor without legal basis pursuant Article 6 (1) of Regulation (EU) 2016/679 or contrary to the principles under Article 5 of the same

противоречие с принципите по чл. 5 от същия регламент, в срок един месец от узнаването администраторът или обработващият лични данни ги връща, а ако това е невъзможно или изисква несъразмерно големи усилия, ги изтрива или унищожава. Изтриването и унищожаването се документират.	Regulation, the data controller or processor shall return such data within a period of one month after having become aware of it or, if this is impossible or would involve disproportionate efforts, shall erase or destroy the data. The erasure and destruction shall be documented.
Закон за защита на личните данни Чл. 45 (Нов - ДВ, бр. 17 от 2019 г.) (1) При обработването на лични данни за целите по чл. 42, ал. 1 личните данни трябва да: 1. се обработват законосъобразно и добросъвестно; 2. се събират за конкретни, изрично указани и законни цели и да не се обработват по начин, който е несъвместим с тези цели; 3. са подходящи, относими и да не надхвърлят необходимото във връзка с целите, за които данните се обработват; 4. са точни и при необходимост да са поддържани в актуален вид; трябва да се предприемат всички необходими мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват; 5. се съхраняват във вид, който позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимия за целите, за които те се обработват; 6. се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.	Personal Data Protection Act Article 45 (New, SG No 17 of 2019) (1) Upon the processing of personal data for the purposes referred to in Article 42 (1), the personal data must be: 1. processed lawfully and fairly; 2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; 3. adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed; 4. accurate and, where necessary, kept up to date; every requisite step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; 5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the said data are processed; 6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Закон за защита на личните данни Чл. 56 (2) Администраторът по ал. 1 е длъжен да изтрие личните данни и субектът на данните има право да поиска администраторът да изтрие личните данни, които го засягат, когато обработването нарушава разпоредбите на чл. 45, 49 или 51 или когато личните данни трябва да бъдат изтрити с цел спазване на правно задължение на администратора.	Personal Data Protection Act Article 56 (2) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her where the processing infringes the provisions of Article 45, 49 or 51 or where the personal data have to be erased for compliance with a legal obligation of the controller.
Закон за защита на личните данни Чл. 56 (3) Администраторът коригира или допълва данните по ал. 1 или изтрива данните в случаите по ал. 2 в срока по чл. 53, ал. 3.	Personal Data Protection Act Article 56 (3) The controller shall rectify or complete the data under Paragraph (1) or shall erase the data in the cases under Paragraph (2) within the period referred to in Article 53 (3).
Закон за хазарта Чл. 22 (1) Държавната комисия по хазарта: 1. издава, отказва да издаде, предсрочно прекратява и отнема лицензи за организиране на хазартни игри на и от лицата, които имат право да ги организират в отделни обекти; 2. издава, отказва да издаде, предсрочно прекратява и отнема лицензи на производители и разпространители, осигуряващи сервизна поддръжка, както и на вносители и разпространители, осигуряващи сервизна поддръжка на игрално оборудване; 3. издава и отказва да даде разрешения за извършване на промени в издадени лицензи по т. 1 и 2; 4. приема общи задължителни игрални условия и правила за видовете хазартни игри, за които издава лицензи; 5. приема общи задължителни изисквания за игралните зали, игралните казина, централния пункт и пунктовете за приемане на залози по отношение на	Gambling Act Article 22 (1) The State Commission for Gambling shall: 1. issue, refuse to issue, terminate earlier and revoke licenses for organizing of gambling games to and from the persons authorized to organize them at particular sites; 2. issue, refuse to issue, terminate earlier and revoke licenses of manufacturers and distributors providing service maintenance, and to importers and distributors providing service maintenance of gambling equipment; 3. issue and refuse to issue permits for making amendments to already issued licenses under items 1 and 2; 4. adopt general mandatory gambling conditions and rules for the types of gambling games for which it issues licenses; 5. adopt general mandatory requirements to the gambling halls, casinos, the central point and the points of acceptance of wagers as regards the type of the premises or building, the minimum area, distribution of premises and the required technical equipment for control; 6. adopt general mandatory rules for the organization of activities and financial control over organizing gambling

вида на помещенията или сградата, минималната площ, разпределението на помещенията и необходимото техническо оборудване за контрол; 6. приема общи задължителни правила за организацията на работата и финансовия контрол при организиране на хазартни игри и задължителни образци за счетоводна отчетност за видовете хазартни игри; 7. (изм. - ДВ, бр. 1 от 2014 г., в сила от 01.01.2014 г.) приема общи задължителни технически изисквания за системите за контрол върху хазартните игри и игралното оборудване, както и общи технически и функционални изисквания към игралния софтуер и комуникационното оборудване за онлайн залаганията и игрите чрез други електронни съобщителни средства; 8. утвърждава списък с лаборатории в Република България и в другите държави - членки на Европейския съюз, в другите държави - страни по Споразумението за Европейското икономическо пространство, или в Конфедерация Швейцария, които могат да извършват изпитвания на игрално оборудване и игрален софтуер на комуникационно оборудване; утвърждава изпитани от такива лаборатории типове и модификации на игрално оборудване, които могат да се произвеждат и внасят, за да се експлоатират в страната; 9. утвърждава задължителните образци на билети, фишове, талони и други удостоверителни знаци за участие в хазартни игри съгласно Наредбата за условията и реда за отпечатване и контрол върху ценни книжа (обн., ДВ, бр. 101 от 1994 г.; изм., бр. 38 от 1995 г., бр. 73 от 1998 г., бр. 8 от 2001 г., бр. 54 от 2008 г. и бр. 22 от 2011 г.); 10. (изм. - ДВ, бр. 1 от 2014 г., в сила от 01.01.2014 г., доп. - ДВ, бр. 105 от 2014 г., в сила от 01.01.2015 г.) утвърждава правила за съхранение на информацията за едновременните игрални сесии, направените залози и формирането на печалбите и одобрява системи за	games and mandatory sample forms for accounting purposes for the types of gambling games; 7. (amended, SG No. 1/2014, effective 1.01.2014) adopt general mandatory technical requirements to the systems of control over gambling games and gambling equipment, as well as general technical and functionality requirements to the gaming software and communication equipment for online betting and games via other electronic means of communication; 8. approve a list of laboratories in the Republic of Bulgaria and in the other EU Member States, in the other states signatories to the European Economic Area Agreement, or in the Swiss Confederation, which may make tests of the gambling equipment and gambling software of communication equipment; shall approve types and modifications of such equipment tested by such laboratories that may be manufactured and imported to be operated in this country; 9. approve mandatory samples of tickets, fills, tokens and other signs certifying participation in gambling games pursuant to the Ordinance on the Conditions of and Procedure for Printing and Control over Securities (promulgated in SG, issue 101 of 1994, as amended in issue 38 of 1995, issue 73 of 1998, issue 8 of 2001, issue 54 of 2008 and issue 22 of 2011); 10. (amended, SG No. 1/2014, effective 1.01.2014) approve rules for storage of the information of the simultaneous gambling sessions, the wagers made and the formation of winnings, and to approve systems for automatic submission of information to a server of the National Revenue Agency for the following gambling games - lotteries, pools, lotto, wagers on outcomes of sports competitions and horse and dog races, bets on chance events, bets involving right-guessing of facts, as well as for online betting and games via other electronic means of communication; the systems for online betting and games via other electronic means of communication should ensure online registration of each transaction in the system of the National Revenue Agency according to a procedure and in a manner set forth in the ordinance under Article 6, Paragraph 1, item 4; 11.

автоматизирано подаване на информацията към сървър на Комисията и на Националната агенция за приходите за следните хазартни игри: лотарии, тото, лото, залагания върху резултати от спортни състезания и надбягвания с коне и кучета, залагания върху случайни събития, залагания, свързани с познаване на факти, както и за онлайн залаганията и игрите чрез други електронни съобщителни средства; системите за онлайн залаганията и игрите чрез други електронни съобщителни средства трябва да осигуряват онлайн регистрация на всяка транзакция в системата на Националната агенция за приходите по ред и начин, определени в наредбата по чл. 6, ал. 1, т. 4; 11. утвърждава представените от организаторите на хазартни игри правила по т. 4 - 7; 12. издава инструкции по прилагането на закона; 13. дава становища по искане на други органи; 14. взема решения за определяне на интернет страници, чрез които се организират хазартни игри от лица, които не са получили лиценз по този закон, както и за преустановяване на нарушенията; на страницата си в интернет Комисията създава, обновява и поддържа списък на тези интернет страници; 15. осъществява и други правомощия, изрично предвидени със закон.	approve the rules provided by organizers of gambling games under items 4 - 7; 12. issue guidelines on the implementation of the act; 13. provide statements of opinion upon request by other authorities; 14. make decisions for determining websites through which gambling games are organized by persons that have not been issued licenses under this act as well as for putting an end to violations; on its website the Commissions shall publish, update and maintain a list of these websites; 15. exercise other powers explicitly provided for by law.
Закон за хазарта Чл.22 (4) Решенията по ал. 1, т. 14 се публикуват на интернет страницата на Комисията в деня на издаването им. Лицата, за които тези решения се отнасят, се смятат уведомени в деня на публикуването. Ако в тридневен срок от публикуването лицето не преустанови нарушението, за което е взето решение	Gambling Act Article 22 (4) The decisions under Paragraph 1, item 14, shall be published on the Commission's website on the date of their issuance. Persons whom these decisions concern shall be deemed notified on the date of publication. If within a 3-day term from publication a person does not stop the violation for which a decision was made

по ал. 1, т. 14, Комисията подава искане до председателя на Софийския районен съд да постанови всички предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги, да спрат достъпа до тези интернет страници. Председателят на Софийския районен съд или оправомощен от него заместник-председател се произнася по искането в срок до 72 часа от постъпването му. Издаденото от съда разпореждане се публикува на интернет страницата на Комисията в деня на получаването му. Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, са длъжни да спрат достъпа до съответните интернет страници в срок до 24 часа от публикуване на разпореждането на съда.	under Paragraph 1, item 14, the Commission shall petition the chairperson of the Sofia District Court to decree that all enterprises providing public electronic communications networks and/or services should stop the access to these websites. The chairperson of the Sofia District Court or a deputy chairperson authorised by him/her shall come up with a ruling regarding the petition within 72 hours from its receipt. The ruling issued by the Court shall be published on the website of the Commission on the day of its receipt. The enterprises providing public electronic communications networks and/or services shall be obliged to stop the access to the respective websites within 24 hours from the publication of the court ruling.
Закон за електронната търговия Чл. 13 (1) (Изм. - ДВ, бр. 41 от 2007 г.) При предоставяне на достъп до или пренос през електронна съобщителна мрежа доставчикът на услуги не отговаря за съдържанието на предаваната информация и за дейността на получателя на услугата, ако: 1. не инициира предаването на информацията; 2. не избира получателя на предаваната информация, и 3. не избира или не променя предаваната информация. (2) (Изм. - ДВ, бр. 41 от 2007 г.) Предоставянето на достъп до или пренос през електронна съобщителна мрежа по смисъла на ал. 1 включва автоматично, междинно и временно съхраняване на предаваната информация, извършено единствено с цел осъществяване на преноса през електронна съобщителна мрежа, като информацията не се съхранява за срок, по-дълъг от обикновено необходимия за осъществяването на преноса.	Electronic Commerce Act Article 13 (1) (Amended, SG No. 41/2007) Upon providing access to or transmission trough electronic communication network the service provider shall not be liable for the content of the information transmitted and for the activities of the recipient of the service, if the provider: 1. does not initiate the transmission of the information; 2. does not select the receiver of the information transmitted, and 3. does not select or modify the transmitted information. (2) (Amended, SG No. 41/2007) Providing access to or transmission through electronic communication network referred to in paragraph (1) also covers an automatic, intermediate and transient storage of the transmitted information, as this shall take place for the sole purpose of carrying out the transmission trough the electronic communication network and the information shall not be stored for any period longer than the one that is reasonably necessary for the transmission

Закон за електронната търговия Чл. 14 (1) Доставчик, който предоставя услуги, осигуряващи автоматизирано търсене на информация, не отговаря за съдържанието на извлечената информация, ако: 1. не инициира предаването на извлечената информация; 2. не избира получателя на извлечената информация, и 3. не избира или не променя извлечената информация. (2) Алинея 1 не се прилага, ако информационният ресурс, от който се извлича информацията, принадлежи на доставчика или на свързано с него лице.	Electronic Commerce Act Article 14 (1) A service provider who provides automated search of information shall not be liable for the content of the derived information if the provider: 1. does not initiate the transmission of the derived information; 2. does not select the receiver of the derived information, and 3. does not select or modify the derived information. (2) Paragraph (1) shall not apply if the information resource from which the information is derived belongs to the provider or related to him person
Закон за електронната търговия Чл. 15 (Изм. - ДВ, бр. 41 от 2007 г.) Доставчик на услуги, който пренася информация, въведена от получателя на услугата в електронна съобщителна мрежа, не отговаря за автоматичното, междинното и временното съхраняване на информацията, необходимо за нейното ефективно предаване към други получатели на услугата по тяхно искане, ако: 1. не изменя информацията; 2. спазва изискванията за достъп до информацията; 3. спазва общоприетите правила за актуализация на информацията; 4. правомерно използва общоприетите технологии за получаване на данни за използване на информацията; 5. незабавно премахва информация, която е съхранил, или преустановява достъпа до нея с узнаването на факта, че:	Electronic Commerce Act Article 15 (Amended, SG No. 41/2007) A service provider who transmits information entered by a recipient of the service into a electronic communication network shall not be liable for the automatic, intermediate and temporary storage of such information or for the content of such information, needed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, if the service provider: 1. does not modify the information; 2. complies with conditions for access to the information; 3. complies with rules regarding the update of the information, specified in a manner widely recognized; 4. does not interfere with the lawful use of widely recognized technology to obtain data for the use of the information; 5. acts expeditiously to remove or to disable access to information he has stored upon obtaining an actual knowledge of the fact that: a) the information has been removed from the network of the primary source, or access to it has been disabled, or b) there is an act of a competent state

а) информацията е била отстранена от мрежата на първоначалния източник или достъпът до нея е бил преустановен, или б) е налице акт на компетентен държавен орган за премахване на информацията или преустановяване на достъпа до нея, когато това е установено със закон.	authority that has ordered such removal of the information or disablement of the access to it, when this has been set fort in a law.
Закон за електронната търговия Чл. 16 (1) Доставчик на услуга, представляваща съхраняване на предоставена от получател на услугата информация, не отговаря за нейното съдържание, както и за дейността на получателя на услугата, ако: 1. не е знаел за противоправния характер на дейността или информацията, или 2. не са му били известни фактите или обстоятелствата, които правят дейността или информацията явно противоправна. (2) Алинея 1 не се прилага, ако: 1. получателят на услугата е свързано с доставчика на услугата лице; 2. доставчикът е узнал или е бил уведомен за противоправния характер на информацията или е бил уведомен от компетентен държавен орган за противоправния характер на дейността на получателя и не е предприел незабавни действия за преустановяване на достъпа до нея или за премахването и; това не освобождава доставчика от произтичащо от закон задължение да запази информацията. (3) (Доп. - ДВ, бр. 94 от 2018 г.) По искане на компетентен държавен орган в случаите, установени със закон, доставчикът е длъжен да предостави всяка информация относно получателя на услугата и дейността му, като с оглед на бързината и неотложността на кибератака, киберинцидент или киберкриза комуникацията да става по	Electronic Commerce Act Article 16 (1) A provider of a service, that constitutes storage of information, when such storage takes place at the request of a recipient of the service who has supplied the information, shall not be liable either for the content of the information stored or for the activities of the recipient of the service, if the service provider: 1. does not have an actual knowledge of the unlawful character of the activities or the information, or 2. is not aware of the facts or circumstances from which the unlawfulness of the activities or information is apparent. (2) Paragraph (1) shall not apply if: 1. the recipient of the service is related to the service provider person; 2. the provider has learned or has been informed about the unlawful character of the information or has been informed by a competent state authority about the unlawful character of the activities of the recipient and has not undertook immediate actions to remove or to disable the access to the information; this does not exempt the provider from the derived from a law obligation to save the information. (3) (Supplemented, SG No. 94/2018) Upon a request of any competent state authority in the cases, established by the law, the provider shall be under the obligation to provide any information concerning the recipient of the service and his activities and in view of the swiftness and urgency of a possible cyberattack, cyberincident or cybercrisis, the communication must take place via electronic means that are protected reliably enough. (4) Paragraphs (1) - (3) shall apply, mutatis mutandis, in the cases where

електронен път, достатъчно надеждно защитен. (4) Алинеи 1 - 3 се прилагат съответно и в случаите, когато доставчик на услуги предоставя достъп до чужда информация посредством електронна препратка.	the service provider leaves access to somebody else's information through electronic link.
Закон за електронната търговия Чл. 17 Доставчикът на услуги не е длъжен да извършва наблюдение на информацията, която съхранява, пренася или прави достъпна при предоставяне на услуги на информационното общество, нито да търси факти и обстоятелства, указващи извършването на неправомерна дейност.	Electronic Commerce Act Article 17 The service provider is not obligated either to monitor the information that he stores, transmits or makes accessible when providing services for the information society or to be in search of facts and circumstances that indicate unlawful activities.
Закон за електронната търговия Чл. 18 Разпоредбите на чл. 13 - 17 се прилагат и за доставчици на услуги на информационното общество, предоставяни безплатно.	Electronic Commerce Act Article 18 The provisions of Articles 13 - 17 shall apply also to providers of information society services that are provided free of charge.

Bibliography

English titles

Legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 3.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23.11.1995,

International Convention on the Elimination of All Forms of Racial Discrimination

Appendix to Recommendation No. R (97)20 of the Committee of Ministers to member states on "hate speech"

Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom.

Reports

"Comparative study on blocking, filtering and take-down of illegal internet content", Council of Europe

Comments of Bulgaria on the country report of the "Comparative study on blocking, filtering and take-down of illegal Internet content"

"Blocking, filtering and take-down of illegal internet content", The Swiss Institute of Comparative Law

Strategy Horizont for 2022, Commission for Personal Data Protection

Books

Nunziato, D., Virtual freedom. Net Neutrality and Free Speech in the Internet Age, 1st ed., Stanford, Stanford University Press 2009

Benedek, W., Kettemann, M. Freedom of expression and the internet, Council of Europe Publishing, 2013

Kelsen, Hans. General Theory of Law and State (Harvard University Press 1949)

Digital resources

Commission for Personal Data Protection, Opinion on the application of the right to be forgotten in the context of personal data processing for journalistic purposes, <https://www.cpdp.bg/index.php?p=element_view&aid=2183>,
accessed 20 February 2020

Definition of adequate, Merriam-webster dictionary, <https://www.merriam-webster.com/dictionary/adequate>, accessed 22 February 2020

Comparative study on blocking, filtering and take-down of illegal internet content, <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>, accessed 20 February 2020

Commission for Personal Data Protection, Opinion on the application of the right to be forgotten in the context of personal data processing for journalistic purposes, <https://www.cpdp.bg/index.php?p=element_view&aid=2183>, accessed 25 May 2020

Comparative study on blocking, filtering and take-down of illegal internet content, <https://www.mtitc.government.bg/sites/default/files/comparative_study_on_filtering_blocking_and_take_down_of_internet_content_bg.pdf>, accessed 20 February 2020

Internet Censorship 2020: A Global Map of Internet Restrictions, <https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/>,
accessed 25 February 2020

Case law

Case of Delfi.AS v. Estonia, European Court of Human Rights, Grand Chamber, Application no. 64569/09, 16.06.2015.

Association Ekin v. France, app. no. 39288/98, § 58 (ECHR, 17 July 2001); Editorial Board of Pravoye Delo and Shtekel v. Ukraine, app. no. 33014/05, § 55 (ECHR 5 May 2011)

Judgment of the Court (Grand Chamber), 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González

Case of Handyside v. the United Kingdom

Pendov v. Bulgaria, app. no. 44229/11 (ECHR)

Bulgarian titles

Legislation

The Constitution of the Republic of Bulgaria 1991

Criminal Code 1968

Criminal Procedure Code 2005

Protection against Discrimination Act 2004

Copyright and Neighbouring Rights Act 1993

Personal Data Protection Act 2002

Gambling Act 2012

Electronic Commerce Act 2006

Radio and Television Act 1999

State Gazette №17 of 2019

State Gazette No. 13, issued on the 14 February 2020

Reports

Annual Human Rights Report for 2018 by Bulgarian Helsinki Committee

Bissera Zankova, Report for Bulgaria (Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, Swiss Institute of Comparative Law 20 December 2015)

Veleva, S. Evolution of freedom of speech in Bulgaria after its accession in the European union.

Books

Drumeva, E., Constitutional Law, 2008

Veleva, S., Freedom of Speech, 2020

Digital resources

National council for journalism ethics, Ethical Code of Bulgarian media, <https://mediaethics-bg.org/%d0%b5%d1%82%d0%b8%d1%87%d0%b5%d0%bd-%d0%ba%d0%be%d0%b4%d0%b5%d0%ba%d1%81-2/ >, accessed 20 February 2020

User policy for Economedia forums, <https://www.economedia.bg/forum.php>, accessed 20 February 2020

The Bulgarian domains are administered by a Joint Stock Company, <https://www.imena.bg/tld_user_nam/app.pl?action_key=ac_c1p2d1_to_about_us&frame_key=fr_c1p2_main_frame>, accessed 20 February 2020

Terms and conditions for domain name registration and support in the .bg zone and the sub-zones, <https://www.register.bg/tld_user_reg/documents/en/terms_and_conditions-v4.9.pdf>, accessed 20 February 2020

Decision of Commision of Journalistic Ethics №25, 12/07/2016 ,<РЕШЕНИЕ № 25 12 юли 2016 по жалба вх. № 03-–021/04.05.2016 г. н>, accessed 20 February 2020

Annual Human Rights Report for 2018 by Bulgarian Helsinki Committee, <https://www.bghelsinki.org/media/uploads/annual_reports/annual-bhc-report-2018-issn-2367-6930-bg.pdf,>, accessed 20 February 2020

Ethical Code of Bulgarian media , <http://mediaethics-bg.org/wp-content/uploads/2016/12/%D0%A0%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D0%B5-15-%D0%BE%D1%82-31.05.2016-%D0%A6%D0%B2%D0%B5%D1%82%D0%BE%D0%BC%D0%B8%D1%80-%D0%9D%D0%B5%D0%BD%D0%BE%D0%B2-%D1%81%D1%80%D0%B5%D1%89%D1%83-Plovdiv24-rev.pdf, > accessed 20 February 2020

Nelly Ognynova , Media law website, <https://nellyo.wordpress.com/2015/06/>, accessed 20 February 2020

Case law

Case № 1/1996 of the Constitutional Court of the Republic of Bulgaria

Decision № 7/1996 of the Constitutional Court of the Republic of Bulgaria

Decision of Commision of Journalistic Ethics №25, 12/07/2016

Decision №15 31/05/2016 of the Commission for Journalistic Ethics

Court Decision № 8 of 15 November 2019 under Constitutional Case 4/2019

Case № 882/2013, 26.11.2013 of District Court of Kardzhali

Case № 2996/2017, 15.11.2018 of District Court of Sofia

Case № 10756/2015 from 12.12.2016 of Supreme Administrative Court of Bulgaria

Decision № 7/1996 of Constitutional Court of Bulgaria

ELSA Czech Republic

Contributors

National Coordinator

Barbora Sveykovská

National Academic Coordinator

Barbora Sveykovská

National Researchers

Dominika Bazalová

Marek Brada

Eliška Říhová

National Linguistic Editor

Josef Levy

Introduction

The creation of the internet has changed billions of lives by providing access to a nearly limitless source of information and changing the way we communicate. The invention brought positives, but also negatives. Billions of people on one network mean that not every information or act by users will be morally right, furthermore legal.

Legal boundaries and limitations are also needed for this interconnected space. Freedom of expression is an issue as old as humanity itself. The question, what is a person allowed to write against established rules whether to be religious, political or social is still here. Nowadays, issues are still the old ones, but new ones arose as child abuse material, terrorism, criminality (in particular hate crimes) and national security.

To address these issues, our country as a member of the EU follows the EU regulatory model and relies on an existing legal framework that is not specific to the internet. This potential regulatory gap is supplemented by court decisions, all the way to the constitutional court.

Topics such as Limitations of freedom, blocking and takedown of internet content, grounds for the content to be blocked/filtered or taken down/removed, 'right to be forgotten' or the 'right to delete', and more will be discussed further.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitations of freedom of expression?

The Czech Republic guarantees freedom of expression in Article 17 of the Charter of Fundamental Rights and Freedoms. It states that everybody has the right to freely express their opinion by word, in writing, in the press, in pictures or in any other form, as well as freely to seek, receive and disseminate ideas and information regardless of the frontiers of the State.

Protection against limitations of freedom of expression is guaranteed by the Constitutional Court of the Czech Republic. Case law regarding this topic is mainly about traditional media (newspaper) interfering with privacy or dignity of celebrities. As stated in decisions no. IV. ÚS 154/97, I. ÚS 156/99 and Pl. ÚS 2/10, there must be balance between public interest to receive information and freedom of speech on one hand and protection of privacy on the other. This balance is considered in each case individually, as there is no universal rule that

would possibly apply to every situation. Anybody whose right to freely express their opinions was restricted can file a complaint with the Constitutional Court. Its decisions are not binding, but they are widely respected by lower courts.

Censorship is not permitted in the Czech Republic, under Article 17, par. 3 of the Charter of Fundamental Rights and Freedoms.

The right to information is guaranteed together with the freedom of expression by Article 17, par. 1 of the Charter of Fundamental Rights and Freedoms. It consists of the right to seek and disseminate information as well as the obligation of state organs to provide information on their activity upon request. This obligation is further specified in Act no. 106/1999 Coll. on free access to information. Classified information is not provided unless the person making the request is entitled to access such information. Classified information is defined by Act no. 412/2005 coll. As 'information in any form recorded on any medium, the disclosure or misuse of which may cause harm to the interests of the Czech Republic or may be disadvantageous to this interest, and which is listed in the list of classified information'.

2. What legislation on the issue of blocking and takedown of internet content does your country have?

Since the freedom of expression in all forms is a fundamental right, all interventions must be lawful, appropriate, and necessary within a democratic society.

The Czech Republic is a party of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) and Additional Protocols (CETS No. 181 and 223), the Convention on Cybercrime (CETS No. 185) , that deals mainly with infringements of copyright, computer-related fraud, child pornography and violations of network security, and also the Additional Protocol (CETS No. 189) concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Regarding national legal regulation, there is not a specific Act on blocking or the takedown of internet content in the Czech Republic, therefore general legislation of different fields of law is used.

Depending on the case and grounds on which the content should be taken down, several legal Acts can be used.

Firstly, if the case is related to a breach of privacy or personal rights, Act no. 89/2012 coll., of the Civil code is used, specifically Section 81 et seq.

Protection against interference with personal rights is defined in Section 82 of the Civil Code, which states as follows: 'An individual whose personality rights have been affected has the right to claim that the unlawful interference be refrained from or its consequence remedied'.

Unlawful use of one's image is also regulated by the Civil Code, under Section 84 and 85: 'Capturing the image of an individual in any way that would allow his identity to be determined is only possible with his consent'. The image of an individual may only be distributed with his consent'.

Withdrawal of such consent is regulated by Section 87: 'A person who consented to the use of documents of a personal nature, portraits or audio or video recordings relating to an individual or his expressions of personal nature may withdraw his consent, even where granted for a definite period'.

Privacy is specifically protected by Section 86: 'No one may interfere in the privacy of another without a lawful reason'.

Internet content can also be taken down on the grounds of breach of copyright and other related rights. This area is regulated by Act no. 121/2000 coll. The rightful author can (among other ways of protecting their rights) request the takedown of illegal copies of their work under Section 40, par.1 d).

Last but not least, internet content can be taken down as a result of a criminal offense. Act no. 40/2009 coll., the Criminal code defines crimes such as libel (Section 148), defamation of a nation, race, ethnic or other group of people (Section 355) and incitement to hatred against a group of persons or restriction of their rights and freedoms (Section 356), which can be committed online.

A very specific reason to take down a website can be found in Act no. 186/2016 coll., the Gambling Act, Section 82 states as follows: 'Internet service providers in the Czech Republic are obliged to deny access to the websites listed on the list of websites with unauthorised internet games.'

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

The reasons for which internet content can be taken down go hand in hand with the legal principles and general laws of the Czech Republic. With the freedom of expression guaranteed by the Charter of Fundamental Rights and Freedoms, it is essential that internet content is not being taken down without any violation of some of the Czech laws. As we have answered in the previous question, the takedown of internet content is not covered in one specific legislation, however,

the issues are regulated in various Acts such as the Civil Code, the Criminal Code or the Copyright Code.

Internet content can only be taken down on grounds of breach of law and it is necessary that there always is a state authority that decides whether or not specific content interferes with another person's rights, if it is offensive or if it can be considered a crime.

Takedown of online content in the field of criminal law is regulated by the Penal Code. In the pre-trial stage it is usually the prosecutor who decides if a website is an instrumentality and therefore is to be seized. However, the Police of the Czech Republic holds a significant power as well. Under the Section 79b of the Penal Code where seizing of instrumentalities is regulated, the Police is capable of seizing the instrumentalities even with no consent from the prosecutor if the matter is urgent. The Police must then within the next 48 hours inform the prosecutor who can revoke the decision. Beginning on 1 February 2019, the Police of the Czech Republic has obtained new powers concerning the preservation of evidence, specifically regarding information technologies. If it is necessary for a crime investigation, the Police of the Czech Republic, under Section 7b of the Czech Criminal Penal Code, can order any person to preserve online data from any change and to deny access to data for 90 days with no consent from the prosecutor, if the matter is of great urgency. The problem is that in a virtual space that changes within seconds, the condition of the matter being urgent is not hard to achieve and therefore literally any website is at risk. A criminal investigation is a very delicate process and if there is no consent needed from the prosecutor and therefore no third party is involved to say if this hard precaution is legitimate, it is much easier for the police to make mistakes. 90 days can obviously be destructive for businesses that use their websites as platforms for selling their products. We probably must wait a little longer before we see how the provision will be used by the police. After the trial has begun, it is only the court that decides if a precaution is needed. In the end the court would decide as a part of the judgement if content is to be confiscated.

In the process of breach of copyright law, it is the author who, under the Section 40 of the Copyright Act, has a right to claim recognition of his authorship, prohibition of the exposure of his right, disclosure of details of the breach, remedying the consequences of the infringement, adequate satisfaction and ban on the provision of the service used to infringe the author's right. Author can inform the provider that his right to authorship has been infringed and demand removal of the concerned content. If the provider does not take immediate action, the author is entitled to pursue the claim by judicial process. In the

judgement, the court usually orders the infringer to take down the content and awards damages to the author.

Under civil law, if a person finds themselves harmed on personality rights by online contribution, this person is entitled to take legal action. Once more, the judgement will probably award damages or order the infringer to apologise officially. Takedown of content can be a part of the judgement as well.

Both Copyright and Civil law make the infringer responsible for deleting harmful content. If the infringer decides not to comply with the judgement, they become exposed to the risk of criminal proceedings.

The takedown of a particular website officially and for good is a difficult process in the Czech Republic. The word 'censorship' is viewed very negatively in Czech society and therefore even the state authorities must always be incredibly careful when deciding if it is appropriate and necessary to censor internet content. However, probably every democratic state will agree that there are activities that are dangerous for society and therefore it is reasonable to fight against them. It is the duty of all states to realise where their social values stand and what needs to be done to maintain them without any illegitimate interference with other rights that have to be protected. An example of one such activity is gambling. Although gambling is not illegal in the Czech Republic, it is considered a dangerous bad habit that can destroy a person's life and therefore is not to be in any form supported by the state. It is as well considered to be one of the top fields to launder money. The government of the Czech Republic is officially trying to fight the gambling, so it is at least regulated as much as possible for a democratic society. There have been new restrictions in the field in the recent past, however, there is especially one restriction that can harm the freedom of the internet.

Entering into force on 1 January 2017, the officials of the Czech Republic created the new Gambling Act and it has been a huge source of discussion ever since. According to some individuals, the Act is constantly choosing to prefer the economic benefit of receiving high amounts of taxes instead of sufficient protection of the gamblers considering the threat of addiction. However, especially one provision leaves the society in doubt. Section 82 of the Gambling Act makes the internet service providers liable for illegal gambling content if they would not deny access to an illegal gambling website within 15 days after the website appeared on a government blacklist. Disobedience of the rule can mean a financial fine up to 1,000,000 CZK.

The development of the internet has made it difficult for the state authorities to handle online gambling and there is no doubt that a new regulation was

necessary, especially considering the fact that there has been no solid legal regulation in the field before. The gambling business was in many cases operated by companies with uncertain background, often of foreign origin. Currently, for online gambling to be legal the operator must obtain a licence from the government and according to official statements from the government, 90% of illegal online gambling activities withdrew from the market within the first month after the regulation became effective.

Section 82 has been criticised very loudly by the Czech Pirate Party with support from quite a large part of the Czech society and even by some of the very respected legal experts. The provision in connection to the Gambling Act as a whole has raised many questions and the complaints escalated even more when first gambling businesses to obtain the licence were the largest companies operating gambling activities in the Czech Republic. Concerns about the unfair process of obtaining the licence has been discussed as well since the Gambling act itself is in many provisions unclear and gives power of decisions to a political office - Ministry of Finance. The liability of internet service providers created by the Gambling Act breaks the principle of 'safe harbour' that is widely applied in the Czech legal system, as will be explained in the further chapters. Illegal gambling is a criminal offence under the Section 252 of the Czech Criminal Code with a penalty of up to three years of imprisonment or prohibition of practice. As previously mentioned, there are powerful instruments in hands of the Police of the Czech Republic that can seize online content to preserve evidence in urgent situations and a court order can take down content for good. Therefore, it is a question if such huge power should be given to the government who furthermore transfers the liability to private internet service providers under the threat of a fine.

The situation culminated after 21 members of the Senate of the Czech Republic brought the matter before the Constitutional Court. The senators fearing the consequences of the new legal regulation claimed that the Constitutional Court declares some of the Gambling Act provisions invalid for their direct conflict with the Czech Constitutional law. However, the Constitutional Court did not comply and stated that similar regulations exist in many European countries, and that the case is not to be considered censorship.

Gambling Act however still raises questions. In November 2019 for example, the Czech Pirate Party succeeded to persuade members of the lower chamber of the Czech Parliament to cancel a controversial and unreasonably strict Section 59 of the Gambling Act that meant a serious disadvantage to Czech citizens in

compare to players from other countries and affected especially Poker players that wanted to take part in international tournaments.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

The question of self-regulation must begin with realising how Czech society views basic rights such as the freedom of expression, the right to information etc. As a former part of the Eastern Communist Bloc, the Czech Republic has done its best to once more provide the protection of human rights and it has become a huge theme after the 1989 Velvet Revolution. Citizens of the Czech Republic remember the era of censorship and restrictions and therefore feel hurt when any state authority or even private persons tend to steal their regained freedom. Although this seems very convincing and positive at first, there still is the danger of restrictions waiting for their time to come. Ariel Hochstadt from the project of vpnMentor said in an interview for one of the Czech internet magazines, that the situation considering the freedom of internet in the Czech Republic is good compared to other countries (he however stated that regulation such as the Section 82 of the Gambling Act could mean a hypothetical threat). Hochstadt sees an advantage in a browser only meant for the Czech users called seznam.cz. He warns that it is not only government censorship that we should be worried about, since the internet browsers themselves can be a threat considering the possibility of priority content shown by the browser. Therefore Mr. Hochstadt recommends for people that speak Czech to verify differences between the information reached on google with the ones found on seznam.cz.

As a former communist country, Czech Republic must always be considered a country that suffers from a persisting Russian influence. An army of trolls used by the powerful is becoming more and more involved in the official politics and state affairs and unfortunately it is mostly the social networks that allow them to comment on inside problems and influence the public opinion. It is of course not only Russia, for example the Czech counter-intelligence BIS warns against the growing impact of China from the year 2014. This influence is in our opinion one of the reasons why the power of fake news, that is spreading over the world, is growing. Media, scientists and non-profit organizations are at war with the fake news websites, some of them are trying to fight the problem through education or publishing of lists of the most dangerous fake news websites, that are in many cases known for their direct connection to Russian institutions. However, we believe that the impact of fake news websites is not supposed to be a part of our research. The reason why it is essential to begin with this kind

of introduction is an initiative named 'neleˇ' (can be translated as 'no lie' or 'do not lie') that has been founded in the Czech Republic within the last month. The aim of the initiative, that has already been supported by T-mobile, HBO, or KB (one of the largest Czech banks), is to reduce the impact of fake news websites by speaking to the private business companies and persuading them to limit financial resources of fake news websites by not advertising on them (nelez.cz). One of the founders Mr. František Vrábel said for a Czech media website reflex.cz that 'neleˇ' is here to alarm people about the necessity to solve the situation of the growing power of fake news and that it should be in the interest of companies to only present their business on websites that are not manipulative and do not spread untruthful information. It is currently well known that fake news is a threat and that it has been spreading through Czech society as well as other countries. It is as well true that the lists gathering the dangerous websites are real, impartial and politically neutral. On the other hand, the 'neleˇ' initiative is a private organisation and although its ideas may seem very impressive and honourable, there is no reasonable doubt that an organisation like that holds a potential to be misused in the future. With well solved marketing ideas and especially with support from big business companies lobbying for their interests, an organisation such as that can gain huge power and if it begins to decide which websites are worth reading, that can mean a real threat to the freedom of speech. An organisation, built on the idea of social values spreading the philosophy of helping the world by restricting access to information, is dangerous, although there is no doubt that fighting against fake news is needed in the modern digital age. The question is whether the 'neleˇ' initiative should be considered censorship. We leave this question for the reader to answer.

The other problem considering the question of self-regulation is not up to date yet, in fact, it may take another year or longer before we even know if anything changes. It has currently been only a few months after the European Parliament adopted the Directive (EU) 2019/790 on copyright in the Digital Single Market. Under European law, the Czech Republic has received two years to transpose the Directive to the Czech legal system. However, there have been voices screaming for the Czech Republic not to vote for the Directive and some of the political parties have never stopped trying to get rid of it. One of those parties is the Czech Pirate Party, which has even asked the prime minister of the Czech Republic for support to join Poland and bring the matter before the Court of Justice of the European Union. The executive branch of the Czech Republic has however not reacted to these pleas.

The problematic part of the Directive that many people in the Czech Republic mistrust is the so known Article 13 (although the provision has received the number 17 in the final version of the Directive, it is constantly referred to as Article 13). This provision regulates the liability of internet intermediaries such as Google or Facebook that should be supervising and blocking the content breaching the law of authorship, through usage of internet bots. As has been stated before, the only way internet content can be taken down in the Czech Republic is through a serious violation of the Czech law, usually ordered by one of the Czech courts, with some exceptions of legal powers held by the Police and Government of the Czech Republic. Together with the so-called Article 11 of the Directive (Article 15 in the final version of the Directive) that orders the internet intermediaries to pay royalties to the authors directly, this must be considered a serious threat. Although Article 11 may seem logical at first, it can be very problematic regarding the risk of internet censorship. According to the interview that we have been writing about above, it is well known that internet intermediaries, especially Google, already hold an extreme power that allows them to censor the content by prioritising Articles shown on the internet. Social networks nowadays have become a platform that private persons and politically active individuals use to express their opinions and to share Articles, that are important for creating public awareness. We believe it is very important that the above mentioned internet intermediaries follow rules created by the authorities, so the content is in accordance with the state legal system and legal principles that we all feel are right to be adhered to. Social networks as well created their own rules of forbidden user's conduct that are to be blocked by the networks themselves or even by the users. These rules are considered to work very well internationally. However, it seems very controversial that internet intermediaries could currently be responsible for the obedience of laws of authorship and therefore their enormous power is supposed to grow even more. The prognosis for the future considering the freedom of the internet, especially the dissemination and obtaining of information is currently at risk.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

The Czech Republic does not apply any specific legislation on these rights. Act no. 110/2019 coll., the Personal Data Processing Act, does not impose any further obligations nor grants any more rights than GDPR.

Specific legislation regulates only press, television and radio broadcasting (Acts no. 46/2000 coll. and 231/2001 coll.). When a statement of fact that affects the

honour, dignity or privacy of a natural person, or the name or reputation of a legal person, is published, that person has the right to require the publisher to publish their reply or an additional statement.

The right to be forgotten is limited mostly in connection with criminal proceedings, in order to ensure preservation of evidence. Such limitation is regulated by various Acts, however, the legislation pursues common objectives such as security and defence of the state, protection of persons and property against crime, the search for persons wanted, missing or lost and supervision of the capital market.

The Constitutional Court of the Czech Republic issued a judgement on data retention on 14 May 2019, file no. Pl. ÚS 45/17.

6. How does your country regulate the liability of internet intermediaries?

Act no. 480/2004 coll., governs, inter alia, the rights and obligations of internet service providers.

Hosting providers are not responsible for the content of the website (Section 5, 6), however there are exceptions from this so called 'Safe Harbour' rule.

In case the provider knew or could know (regarding their expertise and circumstances of the case) and that certain content or conduct of a user is illegal.

In case the provider is or became aware of the illegality of content or conduct and has not taken immediate measures to remove the illegal content or stop the illegal behaviour.

In case the provider has direct or indirect decisive influence on the user's activity.

Hosting providers are not obliged to review or actively seek illegal content on their websites, they must act only upon notice or when illegality is more than obvious (exception no. 1). The responsibility for published content mostly remains upon the publisher himself (or herself).

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

The further mentioned 'Reporters Without Borders' report shows current problems that will potentially continue and have a big impact on freedom of expression mainly for media in the next five years (the media is in the hands of a few players, politicians using the fake news defence).

It will be important to follow the changes of the current state after the Directive on copyright in the Digital Single Market will come into force.

As to ISPs, the situation will probably move in a direction of a gradual increase in the number of situations in which liability is found.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in an online environment? If not, what needs to be done to reach such balance?

As previously mentioned, the basic legislation is provided by the documents of the Czech Constitutional law where freedom of expression is guaranteed especially by Article 17 of the Charter of Fundamental Rights and Freedoms. On the other hand, it is defined that every person has a right to maintain his dignity, honour, privacy, religious beliefs, that membership of an ethnic or national group can mean no harm to the person, etc. Providing basic personality rights is one of the main objectives of the Charter. Considering our topic, especially Articles 1, 3, 10, 15, 16, 24 and 25 of the Charter must be taken into consideration. In the field of criminal law hate speech is forbidden under Sections 355 and 356 of the Czech Criminal Code. Section 355 regulates the criminal offence of public defamation of nation, language, race, ethnic group, etc. If an offender commits such crime by an accessible computer network, the highest sentence can mean spending three years in prison. Section 356 describes the crime of hatred instigation towards any nation, race, ethnic or religious group, etc. If the crime is committed by an accessible computer network, the offender will be punished by six months to three years of imprisonment.

For better understanding, we decided to show the reader some examples of the most famous cases within the last years.

8.1. The complainant Otto Chaloupka v. the decision of the Supreme Court of the Czech Republic from 25 June 2014, judgement from 16 June 2015 file number I. ÚS 3018/14

Otto Chaloupka is a former member of the House of Representatives of the Czech Republic. In the year of 2013, he posted on his Facebook profile reacting to a physical assault against a married couple that has been committed by a group of people belonging to the Roma ethnic group. In the post Mr. Chaloupka threatened the Roma ethnic group (not the particular persons who have committed the offence, however the ethnic group in general). 'Decent people have suffered enough of your thefts, aggression, and unlawful demands and more and more advantages. (…) Push even harder and it will snap once. People are standing on the edge so push harder and prepare for the wilderness. I can already hear the screaming. It will make no difference how fast you are able to run', he posted. Mr. Chaloupka has been sentenced to six months of imprisonment and released on one-year probation.

Mr. Chaloupka was unsuccessful even in front of the Constitutional Court in 2015 using his major argument – the post has been released during his presence in the House of Representatives and therefore he cannot be prosecuted due to the indemnity that he holds as the member of the House of Representatives. The Constitutional Court of the Czech Republic was not of the same opinion since Mr. Chaloupka's Facebook post has not been addressed to other members of the House of Representatives and cannot be considered as a part of the parliamentary discussion.

8.2. Michal Kesudis

Second example is more specific, for it is not a classical hate speech case. Hate speech can be defined as public statement expressing hatred against a person or a group, usually considering problems such as ethnicity, nationality, sex, or sexual orientation, etc. (the borders however are not exact as far as a statement is capable to harm a person psychologically, on his rights or dignity, for an unlawful reason seeing only one of the person's attribute). The case of Michal Kesudis from the year of 2014 brings two different problems together – firstly, the problem of publicly expressing opinions about state authorities that in some cases can be defined as diluting of authority through hatred, aggression and fake news, and secondly, a public approval of criminal offence which is a crime under Section 365 of the Criminal Code. Mr. Kesudis posted on his Facebook profile reacting on a suicide attack against the Czech military forces in Afghanistan. Mr. Kesudis then copied the post to the official profile of the Army of the Czech Republic. In the post Mr. Kesudis endorsed the death of four Czech soldiers

who he referred to as mercenaries. Besides that, he stated in the court for example that the officials of the U.S. are acting as Adolph Hitler in 1939. Mr. Kesudis, a member of the Czech Communist party can be considered a conspiracy theorist, whose opinions are in many ways controversial, however, the court decided that these particular statements he made are beyond any borders. The post dilutes the authority of the Army of the Czech Republic, and especially harms the dignity of the fallen soldiers and their families. As hate speech in usual forms, the statement can be as well considered dangerous since it has created a big debate between Mr. Kesudis's loyal followers. Mr. Kesudis has accepted the sentence of one year on a 30-month long probation.

8.3 The case of the Primary School 'Plynárenská' in Teplice

One of the most observed cases of hate speech of the last years is the case of the Primary School 'Plynárenská' in Teplice (a city in the North of the Czech Republic). The situation began in the year 2017 with an innocent photograph illustrating pupils of the first class in the above-mentioned school which went viral after its release in the local newspaper. It is unfortunately the main point of the problem that the pupils mostly belong to the Roma, Arab and Vietnamese ethnic groups. After the appearance of the photograph on social networks, some individuals began to post comments that we believe are not necessary to be translated for their highly racist and offensive content. The criminal proceedings with three individuals accused of criminal offences has not been concluded yet since the third of the accused has not received the final judgement and is currently to be tried by the District Court again. The other two offenders have been sentenced to imprisonment on probations and financial fines.

These three cases are most certainly not the only ones decided so far or to be decided in the immediate future, however, we are of the opinion that they illustrate the situation in the Czech Republic very well. Freedom of expression as one of the basic political rights often does not correspond with the claims for personality rights protection. To give an example, there have been many disputes between journalists and natural or even legal persons who sued journalists for discharging dignity and other personality rights. However, we believe that this is not to be a part of our research since media communication does not only happen on the internet. It is the social networks that must be discussed and therefore we first need to understand how they work and how we should handle the fact that everybody is suddenly capable of expressing opinions in a way that can influence a large group of people.

We believe that although the freedom to express opinions on social networks has not been fully understood yet, the content of a statement is the major point

that can make a person responsible for hate speech behaviour. It is hard or even impossible to make a specific rule determining exactly how dangerous and able to harm a statement is in general. Therefore, we believe that the case law is and will be the main source of information. The three above mentioned cases show that Czech courts respect guaranteed personality rights that belong to everyone regardless of any personal attributes of being, looking or thinking differently. However, we must as well point to the negatives. Open and free space of social networks unfortunately hosts users that express their hate every single day. It is incredibly sad to see how many people in the Czech Republic use social networks to behave racist, xenophobic, homophobic, etc. We all saw it many times in our lives. Unfortunately, not all these cases end up being punished.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

The balance between allowing freedom of expression online and protecting other rights is always hard to achieve. We believe that freedom of expression is a common theme before even the High Court and is according to our research, very well protected.

To improve the balance between allowing freedom of expression online and protecting other rights, effective enforcement and judicial system must be in place.

Considering our analysis and the common practice of the courts, improvements to encourage the preventive function of law can be made. Firstly, it has become economically advantageous to publish slander and defame because the amount of monetary satisfaction granted is overall low, but recent judgment as in *Havlová v. Bauer Media* (4 mil. Czech crown awarded, currently on appeal) can signal a change. Insufficient awards are in contrast with the preventative function of the law. Secondly, the court rulings take too long. This is proven to be especially problematic in cases when even an immediate decision is too late. The situation is, therefore, more about the objections to the method of judicial decisions rather than about the wording of the legislation.

10. How do you rank the access to freedom of expression online in your country?

The Press Freedom Index can help us in this evaluation. The Press Freedom Index is an annual ranking which evaluates Media independence, environment and self-censorship, legislative framework, transparency, and the infrastructure of countries, compiled and published by Reporters Without Borders.

The positive 13th place that the Czech Republic occupied in 2015 contrasts with the current 40th place for 2019. This fall may be attributed to the influence of top politicians, such as President Milos Zeman, who showed up at a press conference in October 2017 with a dummy Kalashnikov with the inscription 'for journalists' and also due to the level of media ownership concentration, which is reaching critical levels.

Therefore, access is shrinking mainly for journalists.

11. How do you overall assess the legal situation in your country regarding internet censorship?

We believe that despite some individual concerns that we have mentioned in our contribution, the situation in the Czech Republic can be considered as good, or at least we can state that we are not facing any real threats concerning the implementation of internet censorship in the nearest future. Some of the problems that we are dealing with, such as the growing impact of fake news, are known worldwide and therefore cannot be feared in the Czech Republic as something new, invented by the Czech state authorities to restrict the freedom of expression and the right to information. However, it needs to be stated that according to the current political situation in the Czech Republic, new difficulties have appeared that are to be decided in the future. As a result of massive development of social media, people received an unlimited source for seeking information and it is a problematic question, if the connection between the people and the world is not too tight. People do not know what to believe anymore and that is in our opinion one of the reasons why some citizens of the Czech Republic tend to adopt extremist opinions. The media platforms in the Czech Republic are largely controlled by powerful politically involved individuals and the political parties are not afraid to use their posts on social networks as weapons to interact with potential followers. Therefore, independent journalists are in many cases not able to interview important political figures since they simply do not need to answer in order to be seen by the people anymore. This creates information censorship on its own.

However, all of these are themes to be discussed within political sciences, sociology and other sciences before they can (if ever) be regulated by law. Seen from the point of the current Czech legal system itself, legislation is not a problem in the Czech Republic. We have written about the Gambling Act, nevertheless, the theme of gambling probably can justify the government's effort. It is essential that every person who feels adversely affected can bring an action before court that will decide about his claim. It is as well essential that special rules exist for criminal investigations and criminal proceedings that ensure the impartiality and independence of the state authorities. Therefore, we are happy to state once more that the Czech legal system regarding internet censorship can be considered as good.

Conclusion

In our research we focused on the assessment of legislation in the Czech Republic, as well as the current problems and important topics discussed in the Czech media. We explained that freedom of expression, the right to information and other similar relevant basic rights are guaranteed as a part of our constitutional legislation. We then gave examples of the most important international conventions and national Acts that regulate the problems concerning freedom of the internet. We as well tried to explain on what ground can internet content be taken down and discovered that it only can happen in accordance with the Czech legal system and that it is important that there always is a state authority that decides if the internet content is dangerous or holds any wounding potential. Then we showed topics that are widely discussed in the Czech society nowadays and that we believe are capable of harming freedom of the Czech internet. We answered that the right to be forgotten is not applied through any specific legislation, however it is limited mostly in connection to criminal proceedings. According to our research the liability of internet intermediaries currently only includes the so called 'safe harbour' rule. The vision for the future however is not certain, especially for the freedom of speech in connection with media and the right to information, in connection with the new Directive on copyright in the Digital Single Market, is currently at risk. We provided examples of adjudicated cases concerning hate speech and discovered that the judiciary of the Czech Republic has a stable opinion and is doing well in protecting the rights of individuals. However, we expressed the opinion that some changes must come anyway, in order to provide full and especially fast judicial protection of the above-mentioned rights. In the last questions we mentioned problems especially concerning the political situation in the Czech Republic that shrunk the access to freedom of expression for journalists.

Table of legislation

Provision in Czech language	**Corresponding translation in English**
Listina základních práv a svobod, článek 17: (1) Svoboda projevu a právo na informace jsou zaručeny. (2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu. (3) Cenzura je nepřípustná. (4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. (5) Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon.	Charter of Fundamental Rights and Freedoms, Article 17: (1) Freedom of expression and the right to information are guaranteed. (2) Everybody has the right to express freely his or her opinion by word, in writing, in the press, in pictures or in any other form, as well as freely to seek, receive and disseminate ideas and information irrespective of the frontiers of the State. (3) Censorship is not permitted. (4) The freedom of expression and the right to seek and disseminate information may be limited by law in the case of measures essential in a democratic society for protecting the rights and freedoms of others, the security of the State, public security, public health, and morality. (5) Organs of the State and of local self-government shall provide in an appropriate manner information on their activity. The conditions and the form of implementation of this duty shall be set by law.
Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat	Treaty no. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Úmluva o kyberkriminalitě	Treaty no. 185, Convention on Cybercrime
Zákon č. 89/2012 Sb., občanský zákoník, paragraf 81: (1) Chráněna je osobnost člověka včetně všech jeho přirozených práv. Každý je povinen ctít svobodné rozhodnutí člověka žít podle svého. (2) Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.	Act no. 89/2012 Coll., the Civil Code, Section 81: (1) Personality of an individual including all his natural rights are protected. Every person is obliged to respect the free choice of an individual to live as he pleases. (2) Life and dignity of an individual, his health and the right to live in a favourable environment, his respect, honour, privacy and expressions of personal nature enjoy particular protection.

Zákon č. 89/2012 Sb., občanský zákoník, paragraf 82: (1) Člověk, jehož osobnost byla dotčena, má právo domáhat se toho, aby bylo od neoprávněného zásahu upuštěno nebo aby byl odstraněn jeho následek. (2) Po smrti člověka se může ochrany jeho osobnosti domáhat kterákoli z osob jemu blízkých.	Act no. 89/2012 Coll., the Civil Code, Section 82: (1) An individual whose personality rights have been affected has the right to claim that the unlawful interference be refrained from or its consequence remedied. (2) After the death of an individual, the protection of his personality rights may be claimed by any of his close persons.
Zákon č. 89/2012 Sb., občanský zákoník, paragraf 83: (1)Souvisí-li neoprávněný zásah do osobnosti člověka s jeho činností v právnické osobě, může právo na ochranu jeho osobnosti uplatnit i tato právnická osoba; za jeho života však jen jeho jménem a s jeho souhlasem. Není-li člověk schopen projevit vůli pro nepřítomnost nebo pro neschopnost úsudku, není souhlasu třeba. (2)Po smrti člověka se právnická osoba může domáhat, aby od neoprávněného zásahu bylo upuštěno a aby byly odstraněny jeho následky.	Act no. 89/2012 Coll., the Civil Code, Section 83: (1) If an unlawful interference with the personality rights of an individual is associated with his activities in a legal person, the right to the protection of his personality rights may also be asserted by that legal person; however, during his life, the legal person may do so only in the name of the individual and with his consent. If an individual is unable to express his will due to his absence of or inability to reason, consent is not required. (2) After the death of an individual, a legal person may claim that the unlawful interference be refrained from and its consequences remedied.
Zákon č. 89/2012 Sb., občanský zákoník, paragraf 84: Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.	Act no. 89/2012 Coll., the Civil Code, Section 84: Capturing the image of an individual in any way that would allow his identity to be determined is only possible with his consent
Zákon č. 89/2012 Sb., občanský zákoník, paragraf 85: (1)Rozšiřovat podobu člověka je možné jen s jeho svolením. (2)Svolí-li někdo k zobrazení své podoby za okolností, z nichž je zřejmé, že bude šířeno, platí, že svoluje i k jeho rozmnožování a rozšiřování obvyklým způsobem, jak je	Act no. 89/2012 Coll., the Civil Code, Section 85: (1) The image of an individual may only be distributed with his consent. (2) If anyone consents to having his image captured under circumstances which make it evident that the image will be

mohl vzhledem k okolnostem rozumně předpokládat.	distributed, he is conclusively presumed to also consent to its reproduction and distribution in the usual way, as he could reasonably expect under the circumstances.
Zákon č. 89/2012 Sb., občanský zákoník, paragraf 86: Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.	Act no. 89/2012 Coll., the Civil Code, Section 86: No one may interfere in the privacy of another without a lawful reason. Without an individual's consent, it shall in particular be prohibited to intrude into his private premises, watch or record his private life on audio or video recordings, use such or other recordings made by a third person about the private life of an individual, or distribute such recordings about his private life. Private documents of personal nature are protected to the same extent.
Zákon č. 89/2012 Sb., občanský zákoník, paragraf 87: (1)Kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se člověka nebo jeho projevů osobní povahy, může svolení odvolat, třebaže je udělil na určitou dobu. (2)Bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající škodu z toho vzniklou osobě, které svolení udělil.	Act no. 89/2012 Coll., the Civil Code, Section 87: (1) A person who consented to the use of documents of a personal nature, portraits or audio or video recordings relating to an individual or his expressions of personal nature may withdraw his consent, even where granted for a definite period. (2) If consent granted for a definite period is withdrawn without it being justified by a substantial change in circumstances or any other reasonable cause, the withdrawing person shall compensate the person to whom he granted the consent to the resulting damage.
Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), paragraf 40, odstavec 1, písmeno d: Autor, do jehož práva bylo neoprávněně zasaženo nebo jehož právu hrozí	Act no. 121/2000 Coll. on copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act), Section 40, Subsection 1, d: An author whose right has been unjustifiably infringed or whose right is in

neoprávněný zásah, může se domáhat zejména: 1. stažením neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky podle § 43 odst. 2 z obchodování nebo jiného užití, 2. stažením z obchodování a zničením neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky podle § 43 odst. 2, 3. zničením neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky podle § 43 odst. 2, 4. zničením nebo odstraněním materiálů a nástrojů použitých výlučně nebo převážně k výrobě neoprávněně zhotovené rozmnoženiny či napodobeniny díla nebo zařízení, výrobku nebo součástky	danger of being unjustifiably infringed may claim in particular: 1.withdrawal of an unauthorized reproduction or imitation of a work or equipment, product or component pursuant to Section 43 (2) from trading or other use, 2. withdrawal from trade and destruction of an unauthorized reproduction or imitation of a work or equipment, product or component pursuant to Section 43, Paragraph 2, 3. destruction of an unauthorized reproduction or imitation of a work or equipment, product or component pursuant to Section 43, Paragraph 2, 4. destruction or disposal of materials and tools used exclusively or principally to produce an unauthorized reproduction or imitation of a work or equipment, product or component.
Zákon č. 40/2009 Sb., trestní zákoník, paragraf 355: (1)Kdo veřejně hanobÍ a)některý národ, jeho jazyk, některou rasu nebo etnickou skupinu, nebo b)skupinu osob pro jejich skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že jsou skutečně nebo domněle bez vyznání, bude potrestán odnětím svobody až na dvě léta. (2)Odnětím svobody až na tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a) nejméně se dvěma osobami, nebo b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.	Act no. 40/20009 Coll., Criminal Code, Section 355: (1) Whoever publically defames a) any nation, its language, any race of ethnic group, or b) a group of people for their true or presupposed race, belonging t an ethnic group, nationality, political or religious beliefs or because they are truly or supposedly without religion, shall be sentenced to imprisonment for up to two years (2) An offender shall be sentenced to imprisonment for up to two years, if he/she commits the act referred to in Sub-section (1) a) with at least two persons, or b) by press, film, radio, television, publically accessible computer network or in another similarly effective way

Zákon č. 40/2009 Sb., trestní zákoník, paragraf 356: (1)Kdo veřejně podněcuje k nenávisti k některému národu, rase, etnické skupině, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků, bude potrestán odnětím svobody až na dvě léta. (2)Stejně bude potrestán, kdo se spolčí nebo srotí k spáchání činu uvedeného v odstavci 1. (3)Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, a) spáchá-li čin uvedený v odstavci 1 tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo b)účastní-li se aktivně takovým činem činnosti skupiny, organizace nebo sdružení, které hlásá diskriminaci, násilí nebo rasovou, etnickou, třídní, náboženskou nebo jinou nenávist.	Act no. 40/20009 Coll., Criminal Code, Section 356: (1) Whoever publically instigates hatred towards any nation, race, ethnic group, religion, class or another group of people or instigates suppression of rights and freedoms of their members, shall be sentenced to imprisonment for up to two years. (2) The same sentence shall be imposed to anyone who conspires or assembles to commit the act referred to in Sub-section (1). (3) An offender shall be sentenced to imprisonment for six months to three years, if he/she a) commits the act referred to in Sub-section (1) by press, film, radio, television, publically accessible computer network or in another similarly effective way, or b) actively participates in activities of a group, organisation or association that promotes discrimination, violence or race, ethnical, class, religious or other hatred by such an act
Zákon č. 186/2016 Sb, o hazardních hrách, paragraf 82: Blokace nepovolených internetových her (1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami (dále jen „seznam nepovolených internetových her").	Act no. 186/2016 Coll. on gambling, Section 82: Block unauthorized internet games (1) Internet connection providers in the Czech Republic are obliged to prevent access to websites listed on the list of websites with unauthorized internet games (hereinafter referred to as the 'list of unauthorized internet games').

(2) Na seznam nepovolených internetových her se zapíše internetová stránka, na níž je provozovaná internetová hra v rozporu s § 7 odst. 2 písm. b). (3) Povinnost podle odstavce 1 jsou poskytovatelé připojení k internetu povinni splnit ve lhůtě 15 dní ode dne zveřejnění internetové stránky v seznamu nepovolených internetových her.	(2) The website on which the internet game is operated in conflict with § 7 para. 2 let. b). (3) Internet service providers are obliged to fulfill the obligation pursuant to paragraph 1 within 15 days from the date of publication of the website in the list of unauthorized internet games.
Směrnice Evropského Parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES	Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market
Zákon č. 1/1992, Ústava České republiky, článek 1: (1) Česká republika je svrchovaný, jednotný a demokratický právní stát založený na úctě k právům a svobodám člověka a občana. (2) Česká republika dodržuje závazky, které pro ni vyplývají z mezinárodního práva.	The Charter of the Czech Republic, Act no. 1/1993 Coll., Article 1: (1) The Czech Republic is a sovereign, unitary, and democratic state governed by the rule of law, founded on respect for the rights and freedoms of man and of citizens. (2) The Czech Republic shall observe its obligations resulting from international law.
Zákon č. 1/1992, Ústava České republiky, článek 10: Vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, jsou součástí právního řádu; stanoví-li mezinárodní smlouva něco jiného než zákon, použije se mezinárodní smlouva.	The Charter of the Czech Republic, Act no. 1/1993 Coll., Article 10: Promulgated treaties, to the ratification of which Parliament has given its consent and by which the Czech Republic is bound, form a part of the legal order; if a treaty provides something other than that which a statute provides, the treaty shall apply.

Bibliography

English titles

Legislation

Charter of Fundamental Rights and Freedoms

Act no. 106/1999 Coll. On Free Access to Information

Treaty no. 108, Convention for the Protection of Individuals regarding Automatic

Processing of Personal Data

Treaty no. 185, Convention on Cybercrime

Act no. 89/2012 Coll., the Civil Code

Act no. 121/2000 Coll. on copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act)

Act no. 40/20009 Coll., Criminal Code

Act no. 186/2016 Coll. on gambling

Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market

Act no. 110/2019 Coll. (Personal Data Processing Act)

Act no. 46/2000 Coll. (Press Act)

Act No. 231/2001 Coll., on Radio and Television Broadcasting Operation and on Amendments to Other Act

Act No. 480/2004 Coll., on Certain Information Society Services

Act No. 141/1961 Coll., Criminal Procedure Code

Reports

Annual Report of the Security Information Service for 2014 <https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2014-vz-cz.pdf>, accessed 28 May 2020

Ranking 2020, 2020 World Press Freedom Index <https://rsf.org/en/ranking>, accessed 28 May 2020

Periodicals

Petr Málek, 'The case about the first-graders from the primary school in Teplice is back in court' (2019) Teplický deník <https://teplicky.denik.cz/zlociny-a-soudy/kauza-okolo-teplicke-skoly-zs-plynarenska-je-zpet-u-soudu-20190426.html>, accessed 27 May 2020

'On Facebook he approved the attack on Czech soldiers. He was given a probation for a vulgar comment.' (31 August 2015), Hospodářské noviny <https://domaci.ihned.cz/c1-64533320-na-facebooku-schvaloval-utok-na-ceske-vojaky-za-vulgarni-komentar-dostal-podminku>, accessed 28 May 2020

Tomáš Weiss, 'Online gambling regulation works' (22 October 2019), Ministry of Finance of the Czech Republic <https://www.mfcr.cz/cs/aktualne/v-mediich/2019/regulace-on-line-hazardu-funguje-36414>, accessed 28 May 2020

Čestmír Strakatý 'Analyst Vrábel: We want to deprive disinformation sites of money, we have evidence against them, but Facebook is even worse' (11 Februrary 2020), Reflex <https://www.reflex.cz/clanek/prostor-x/99697/analytik-vrabel-dezinformacni-weby-chceme-pripravit-o-penize-mame-proti-nim-dukazy-facebook-je-ale-jeste-horsi.html>, accessed 28 May 2020

Renáta Bohuslavová, 'Greed and clientelism, the gambeling law is lobbed, the Pirates are angry' (28 February 2017), Echo24 <https://www.echo24.cz/a/iGT4S/hamiznost-a-klientelismus-zakon-o-hazardu-je-zlobbovany-zlobi-se-pirati>, accessed 28 May 2020

Digital resources

Aram Sargsyan, Tereza Havlíčková, 'Internet censorship - is there a place for it in the Czech legal system since 1 February 2019?' (17 May 2019), eprávo.cz <https://www.epravo.cz/top/clanky/cenzura-internetu-je-pro-ni-od-1-unora-2019-v-ceskem-pravnim-radu-misto-109333.html>, accessed 28 May 2020

'Gambling regulation works, the state deals with the transfer of gambling to the Internet' (5 November 2019), Government of the Czech Republic <https://www.vlada.cz/cz/media-centrum/aktualne/regulace-hazardu-funguje--stat-se-zabyva-presunem-hrani-na-internet-177498/>, accessed 28 May 2020

Everything about Apple, 'How is the Czech Republic doing with internet freedom and censorship? We bring you an interview with a leading expert in this field' (6 July 2017) <https://www.letemsvetemapplem.eu/2017/07/07/ceska-republika-internet-cenzura/>, accessed 28 May 2020

Tereza Brhelová, Zdislava Pokorná, 'The Copyright Directive is unconstitutional, it should be resolved by a court, Pirates claim and ask Babiš for support' (6 September 2019), Seznam <https://www.seznamzpravy.cz/clanek/smernice-o-autorskem-pravu-je-protiustavni-mel-by-ji-resit-soud-tvrdi-pirati-a-zadaji-babise-o-podporu-78489>, accessed 28 May 2020

'Is there a risk of censorship? The founders of the Internet warn against the Copyright Directive' (5 September 2018), Novinky.cz <https://www.novinky.cz/internet-a-pc/clanek/hrozi-cenzura-zakladatele-internetu-varuji-pred-smernici-o-autorskem-pravu-40067691>, accessed 29 May 2020

Petr Cieslar, Markéta Paráčková, 'The free internet ends. And we don't even know about it' (21 June 2018) <https://www.studenta.cz/life/svobodny-internet-konci-a-ani-o-tom-nevime/r~23b503dc754211e8aa580cc47ab5f122/>, accessed 29 May 2020

Vít Šimánek, 'Martin Konvička's persecution for "Muslims in meat-and-bone meal" is over. It was stopped by the plaintiff' (14 May 2018), Česká televize <https://ct24.ceskatelevize.cz/domaci/2478376-stihani-martina-konvicky-za-masokostni-moucku-skoncilo-zastavil-ho-statni-zastuoce>, accessed 29 May 2020

Case law

Judgement of the Constitutional Court Pl. ÚS 45/17

Judgement of the Constitutional Court III. ÚS 3844/13

Judgement of the Constitutional Court Pl. ÚS 28/16

Judgement of the Constitutional Court I. ÚS 3018/14

Czech titles

Legislation

Listina základních práv a svobod

Zákon č. 106/1999 Sb. o svobodném přístupu k informacím

Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat

Úmluva o kyberkriminalitě

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 186/2016 Sb, o hazardních hrách

Směrnice Evropského Parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon)

Zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů

Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

Zákon č. 141/1961 Sb., o trestním řízení soudním

Reports

Výroční zpráva Bezpčnostní informační služby za rok 2014 <https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2014-vz-cz.pdf>, accessed 28 May 2020

Ranking 2020, 2020 World Press Freedom Index <https://rsf.org/en/ranking>, accessed 28 May 2020

Periodicals

Petr Málek, 'Kauza okolo prvňáčků z teplické školy ZŠ Plynárenská je zpět u soudu' (2019) Teplický deník <https://teplicky.denik.cz/zlociny-a-soudy/kauza-okolo-teplicke-skoly-zs-plynarenska-je-zpet-u-soudu-20190426.html>, accessed 27 May 2020

'Na Facebooku schvaloval útok na české vojáky. Za vulgární komentář dostal podmínku.' (31 August 2015), Hospodářské noviny <https://domaci.ihned.cz/c1-64533320-na-facebooku-schvaloval-utok-na-ceske-vojaky-za-vulgarni-komentar-dostal-podminku>, accessed 28 May 2020

Tomáš Weiss, 'Regulace on-line hazardu funguje' (22 October 2019), Ministerstvo financí České republiky <https://www.mfcr.cz/cs/aktualne/v-mediich/2019/regulace-on-line-hazardu-funguje-36414>, accessed 28 May 2020

Čestmír Strakatý 'Analytik Vrábel: Dezinformační weby chceme připravit o peníze, máme proti nim důkazy, Facebook je ale ještě horší' (11 Februrary 2020), Reflex <https://www.reflex.cz/clanek/prostor-x/99697/analytik-vrabel-dezinformacni-weby-chceme-pripravit-o-penize-mame-proti-nim-du kazy-facebook-je-ale-jeste-horsi.html>, accessed 28 May 2020

Renáta Bohuslavová, 'Hamižnost a klientelismus, zákon o hazardu je zlobbovaný, zlobí se Piráti' (28 February 2017), Echo24 <https://www.echo24.cz/a/iGT4S/hamiznost-a-klientelismus-zakon-o-hazardu-je-zlobbovany-zlobi-se-pirati>, accessed 28 May 2020

Digital resources

Aram Sargsyan, Tereza Havlíčková, 'Cenzura internetu – je pro ni od 1. února 2019 v českém právním řádu místo?' (17 May 2019), eprávo.cz <https://www.epravo.cz/top/clanky/cenzura-internetu-je-pro-ni-od-1-unora-2019-v-ceskem-pravnim-radu-misto-109333.html>, accessed 28 May 2020

'Regulace hazardu funguje, stát se zabývá přesunem hraní na internet' (5 November 2019), Vláda České republiky <https://www.vlada.cz/cz/media-centrum/aktualne/regulace-hazardu-funguje--stat-se-zabyva-presunem-hrani-na-internet-177498/>, accessed 28 May 2020

Vše o Apple, 'Jak je na tom Česká republika se svobodou internetu a cenzurou? Přinášíme rozhovor s předním expertem v této oblasti' (6 July 2017) <https://www.letemsvetemapplem.eu/2017/07/07/ceska-republika-internet-cenzura/>, accessed 28 May 2020

Tereza Brhelová, Zdislava Pokorná, ' Směrnice o autorském právu je protiústavní, měl by ji řešit soud, tvrdí Piráti a žádají Babiše o podporu' (6 September 2019) Seznam <https://www.seznamzpravy.cz/clanek/smernice-o-autorskem-pravu-je-protiustavni-mel-by-ji-resit-soud-tvrdi-pirati-a-zadaji-babise-o-podporu-78489>, accessed 28 May 2020

'Hrozí cenzura? Zakladatelé internetu varují před směrnicí o autorském právu' (5 September 2018), Novinky.cz <https://www.novinky.cz/internet-a-pc/clanek/hrozi-cenzura-zakladatele-internetu-varuji-pred-smernici-o-autorskem-pravu-40067691>, accessed 28 May 2020

Petr Cieslar, Markéta Paráčková, 'Svobodný interent končí. A ani o tom nevíme' (21 June 2018) <https://www.studenta.cz/life/svobodny-internet-konci-a-ani-o-tom-nevime/r~23b503dc754211e8aa580cc47ab5f122/>, accessed 28 May 2020

Vít Šimánek, 'Stíhání Martina Konvičky za „muslimy v masokostní moučce" skončilo. Zastavil ho žalobce' (14 May 2018), Česká televize <https://ct24.ceskatelevize.cz/domaci/2478376-stihani-martina-konvicky-za-masokostni-moucku-skoncilo-zastavil-ho-statni-zastuoce>, accessed 28 May 2020

Case law

Nález Ústavního soudu Pl. ÚS 45/17

Nález Ústavního soudu III. 3844/13

Nález Ústavního soudu Pl. ÚS 28/16

Nález Ústavního soudu I. ÚS 3018/14

ELSA Finland

Contributors

National Coordinator

Saara Siintola

National Researchers

Ida Lehto

Heidimaria Manninen

Minttu Matikainen

Essi Miettinen

Terhi Raikas

Anna-Mari Saloranta

Matias Stubbe

Roosa Toivonen

Anika Zabeen

National Academic Supervisors

Päivi Korpisaari

Sara Lehtilä

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

1.1. The legal basis of the Finnish freedom of expression

The most important laws in the Finnish legislation concerning the protection of freedom of expression are the Finnish Constitution, and the Act on the Exercise of Freedom of Expression in the Mass Media, which contains more detailed provisions on the exercise of the constitutional freedom of expression in the media. According to the Section 12 of the Finnish Constitution, everyone has a right to the freedom of expression. This entails the right to express, disseminate and receive information, opinions, and other communications without prior intervention by public authority. The Constitution also embodies the principle of democracy and the rule of law.

The application of Freedom of Expression is further secured by the practice of the Constitutional Law Committee. The aforementioned means that the freedom of expression in Finland has a strong constitutional background.

1.2. The legal limitations of freedom of expression

It is central to understand that there is legislation both to protect the freedom of expression and to make limitations towards it. In Article 10 of the European Convention on Human Rights, Freedom of Expression is defined as the freedom to hold opinions and to receive and impart information and ideas without interference by a public authority and regardless of frontiers. Even in democratic societies, the right is not absolute, however. The second paragraph of the Article sets out qualifications for the exercise of the right. The idea is that Freedom to Expression is intertwined with duty and responsibility. The paragraph explicitly allows such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. In many cases, a balancing act is required between Freedom of Expression and other rights and freedoms, such as the right to privacy or the prohibition of discrimination.

Freedom of expression can be limited both legitimately and illegitimately, the line between which is subject to debate. Of the types and forms limitations considered illegitimate, censorship is perhaps the most notable one. It can be

defined as the institution, system or practice of reading communication and deleting material considered sensitive or harmful.[405] As explained, drawing the line between legitimate limitations to freedom of expression and censorship is not an easy task. Censorship could be done out of wish to protect people, for instance from seeing something that they might consider hurtful. In most cases, however, when we speak of censorship it is practices to reinforce specific political or religious agendas that we have in mind – for instance attempts to protect those in power by censoring information which might turn the people against them.

In Finland, all documents and recordings by public authorities are, as a rule, public, unless their publication has for compelling reasons been specifically restricted by an act. This means that everyone has the right to access public documents and recordings, a transparency tool which effectively limits the possibility of censorship and upholds the fulfilment of Freedom of Expression in the country.

1.3. Freedom of expression in Finnish case law

The fulfilment of Freedom of Expression in Finland has been excellent for many years. 'The land of the free press' has consistently ranked among the best in the Press Freedom Index, a comprehensive report published annually by Reporters Without Borders. The index evaluates the independence and pluralism of media, free flow of information, legality, security, and freedom of authors.[406]

One good example to demonstrate the strong status of freedom of expression and the role of journalists in Finland is a case by the District Court of Helsinki in October 2019. The court handed heavy sentences to two pro-Putin activists for defaming and stalking a female journalist with the purpose of trying to silence her. The court drew the line that extreme hate speech cannot hide behind the right to Freedom of Expression.[407] The same year, Finland was ranked the second-best country in the World Press Freedom Index.[408]

1.4. Limitations to freedom of expression and the Finnish Criminal Code

All limitations to the Freedom of Expression are not considered censorship or problematic. The Freedom of Expression does not entail that anything can be

405 Merriam-Webster dictionary <https://www.merriam-webster.com/dictionary/censorship> accessed 10 June 2020.

406 Reporters without borders: 2020 World Press Freedom index <https://rsf.org/en/ranking> Accessed 10 June 2020.

407 Reporters Without Borders: Finland <https://rsf.org/en/finland> accessed 10 June 2020.

408 Reporters Without Borders: 2019 World Press Freedom Index – A cycle of fear <https://rsf.org/en/2019-world-press-freedom-index-cycle-fear> accessed 10 June 2020.

said or done without consequences. The prohibition of hate speech – which would entail a limitation of the Freedom of Expression - has in recent years been a political hot potato in the Finnish news media. Hate speech has no legal definition in Finland, and the contents of the concept in the general public debate and language use are somewhat ambiguous.

From a legal point of view, it is central to understand that there is already legislation in place which criminalises many forms of hate speech and comparable harmful expressions.

The Finnish Criminal Code contains two types of crimes which effectively limit the Freedom of Expression: defamation and ethnic agitation. Both acts are punishable by a fine or imprisonment, depending on the seriousness of the crime in each individual case. The main difference between the two is that the target of defamation is an identifiable individual, whereas ethnic agitation is targeted at a group based on a factor such as race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation, or disability.

It is also noteworthy that the commission of any criminalised offence for a motive based on race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or another corresponding ground is grounds for increasing the punishment under Chapter 6, section 5 of the Criminal Code. This can be thought to increase the protection of vulnerable groups against hate speech and silencing even in cases where the criteria for defamation or ethnic agitation are not fulfilled.

2. Which legislation on the issue of blocking and takedown of Internet content does your country have?

2.1. General overview of the Finnish System of blocking and takedown

The Finnish legal system is based on the civil law and Nordic legal traditions, in which sources of law are to a high degree systematised in legislation. Sources of law can be roughly divided into three categories according to the strength of their binding effect in judicial interpretation: strongly binding sources, weakly binding sources, and permitted sources. Strongly binding sources of law include statutory law and established custom, weakly binding norms legal praxis of the Supreme Court and the Supreme Administrative Court as well as legislative drafts. The permitted sources include e.g. jurisprudence, legal principles, and research literature.[409] The underpinning principle of doctrine of precedent in

[409] Aarnio, Laintulkinnan teoria, 1989, 220-221.

common law countries has less importance in Finland, even if the precedents set by the Supreme Court and Supreme Administrative Court are of considerable practical importance. The interpretation of Finnish law and judicial decisions are hugely influenced by relevant EU law and human rights law, as well as national administrative norms and practices.

The international human right treaties binding Finland and Section 12 of the Finnish Constitution (731/1999) on the Freedom of Expression set the frame for Internet content restrictions. The national definition of the Freedom of Expression does not entail any specific technical measures, meaning that the same rules apply for both traditional media and Internet media. Most importantly, according to the Section 12 of the Finnish Constitution, preliminary (*ex ante*) restrictions of the right are prohibited. Thus, in principle, Internet content shall not be restricted beforehand, and the actions taken should be done afterwards the content is provided. It must be noted that virtual private networks (VPNs) are not prohibited by law.

The relevant legislation does not typically require specific technical measures for restricting illegal content. Filtering, blocking and take-down are not usually mentioned separately as specific means to restrict content. The Act on Services in Electronic Communications (7.11.2014/917) sets general procedures to block, filter and take-down of illegal Internet content. However, the definition of prohibited content is spread out to several different national norms. Some examples of the said legislation include:

- The Criminal Code of Finland (39/1889)
- The Copyright Act (404/1961), the Patents Act (550/1967), the Trademarks Act (544/2019)
- Act on the Exercise of Freedom of Expression in Mass Media (460/2003)
- The Data Protection Act (1050/2018), based on the General Data Protection Regulation 2016/679 (EU))

Typically blocking and take-down of content is ordered by a court (for example, Section 185 of the act on Services in Electronic Communications concerning how a court may order an information society service provider to disable access to information). Exemptions are limited to specific situations, which are governed by the legislation. For example, Internet Service Providers (ISPs) are required to act before a court order when the Internet content is about ethnic agitation, depictions of violence, CAM (child abuse material), sexual violence or

intercourse with an animal in order to be considered free of liability.[410] The liability of Internet intermediaries will be discussed more in depth at the question 6.

2.2. Specific regulation and legal praxis in different sectors

In the following section, mentioned legislation concerns intellectual property rights, security as well as consumer rights and well-being. As mentioned earlier in section 2.1, said legislation must be interpreted in accordance with international treaties, human rights, and the hierarchy of Finnish legal system.

2.2.1. Security and criminal matters

In general, most criminal matters and criminal Internet content are regulated by the Criminal Code of Finland. For example, the Criminal Code regulates the blocking and take-down of terrorist content.

Some regulations include norms concerning take-down of criminal material, but most reference back to the Criminal Code. For example, the Act on the Exercising of Freedom of Expression in Mass Media (13.6.2003/460) states in the Section 18 that a court may order an intermediate to stop a distribution of an online message, if it is obvious from the content of the message that it is punishable to distribute it to the public. The Constitutional Law Committee evaluated that the message must be interpreted as a broad qualification for any online message, which contains criminal material.[411]

Telecommunications operators have an obligation to provide an Internet connection without content-based discrimination. However, legislation includes an exception to this when the content in question concerns CAM.[412] These restrictions can be based on contracts or done under the business freedom.[413] The Act on Preventive Measures for Spreading Child Pornography (1068/2006) is a specific legislation, which states in section 3 that the intermediates have a right to set specific measures to prevent the distribution of CAM.

2.2.2. Consumer rights and consumer well-being

At the moment, Finnish legislation does not include norms which allow online content blocking and take-down based purely on customer rights. However, the official working group on the renovation of the competence of consumer

410 The act on Services in Electronic Communications section 184, the Criminal Code of Finland, chapter 11 section 10, chapter 17 sections 17-18.

411 PeVM 14/2002 vp, 7.

412 HE 99/2006 vp, 12.

413 Pekka Savola, Tekijänoikeus Internetissä – suojaamisen keinot ja strategiat (Oikeus 1/2013 (42) 1 49-70) 64.

authorities has made a legislation proposal. According to the proposal, a competent official could order Internet content to be blocked, taken down or the access to be restricted, if the content could cause serious harm to the general well-being of a consumer.[414]

The advertising of gambling is regulated in Finland (the Finnish Lotteries Act, Section 14 b). There have been cases concerning the restriction of online gambling advertising.[415] According to the Supreme Administrative Court, Finnish officials could prohibit online gambling advertising, when the gambling company did not have a permit in Finland and the advertising was aimed at the Finnish audiences. The court referenced, for example, to the case of European Court of Human Rights (*Hachette Filipacchi Presse Automobile and Paul Dupuy v. France* 5 March 2009), and stated that national health can be a reason to restrict freedom of expression [on the Internet]. Another decision concerning gambling sites was ruled by the Helsinki district court concerning the Apple Store. The district court ordered gambling apps to be deleted from the Finnish webstore.[416]

The preliminary investigation on the legislation of the gambling, concerning the reform of the Lotteries Act, evaluated possibilities to block gambling site IPs.[417] At the moment, Finland has not blocked gambling on foreign websites.[418]

Right to be forgotten is part of the individual's right for informational self-determination. The Data Protection Act, based on the General Data Protection Regulation 679/2016 of EU, mentions a natural person's right to be forgotten. Right to be Forgotten will be discussed more in depth in question 5.

2.2.3. Intellectual property rights

Procedure to protect intellectual property rights on the Internet follows the principles set by the freedom of expression (Section 12 of the Constitution) and protection of ownership (Section 15 of the Constitution). The Finnish Copyright Act, Patents Act and Trademark Act set similar norms concerning protection of intellectual property rights on the Internet and the take-down procedure. According to the Section 60 b-d of the Copyright Act, either an author or their representative can request for a discontinuation order by a court or can request

414 Sofia Asperlund, Katri Kummoinnen, Kuluttajaviranomaisten toimivaltuuksien uudistaminen. (Työryhmän mietintö, oikeusministeriö 2019) 98.

415 Administrative Supreme Court KHO 2018:86. Helsinki district court 8.11.2017. L 16/3002. ECRI Report on Finland (fifth monitoring cycle), <http://rm.coe.int/fifth-report-on-finland/1680972fa7> accessed February 13 2020.

416 See: Knuutila and others, Viha vallassa: Vihapuheen vaikutukset yhteiskunnalliseen päätöksentekoon. (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2019:57).

417 Elina Rydman, Tukia Jukka, Rahapelilainsäädäntöä koskeva esiselvitys. (Sisäministeriön julkaisuja 2019:25) 46-51.

418 ibid 39.

for an interim order. The Patents Act Section 57 b and Trademark Act set similar possibilities for intellectual property right owners. It must be noted that the Section 60 e of the Copyright Act includes a possibility for a blocking order in the case of an unknown infringer. This section was not included in the previous version of the law. According to the draft legislation, one of the reasons for the need to change the law was that intellectual property right owners should be better protected even in the cases where the alleged infringer was abroad or unknown.[419]

The abovementioned content take-down procedure due to intellectual property rights follows the general Finnish principle that take-downs and blockings must be ordered by a court. However, the act on Services in Electronic Communications sets a specific procedure, in which intermediaries can act before a court order in case of a copyright infringement (Section 189). This is an exemption to the mentioned general rule of the court order.

Few recent cases concern Internet blocking and intellectual property rights: the Market Court ordered seven Finnish operators to block customers from assessing websites containing copyright protected material.[420] In another case, the Helsinki district court ordered teleoperators to block access to the Pirate Bay -service.[421] The Court of Appeal set a similar order to another operator.[422]

3. On which grounds may Internet content be blocked/filtered or taken down/removed in your country?

3.1. Unlawful content in criminal law and civil law

In general, Finland has several laws which regulate on which ground Internet content may be allowed or not. Content may be considered 'prohibited content' if it is illegal under Finnish laws, like images and videos of child sexual abuse, content that advocates terrorist acts and content that promotes, incites or instructs in crime or violence.[423] According to the European Convention on Human Rights article 10(2): the protection of national security, territorial integrity, public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, and the

419 HE 181/2014 vp, 25.
420 Market Court MAO 311:18, Market Court MAO 243:16.
421 Decision 28.6.2012 of Helsinki District Court. H 11/48307. Decision 28.6.2012 of Helsinki District Court. H 11/51554.
422 Decision 15.6.2012 of Helsinki Court of Appeal. S 11/3097.
423 For example Finnish Criminal Code Chapter 17 Section 18 and 19, Chapter 24 Sections 8 and 10.

prevention of the disclosure of information received in confidence are the protected interests which can be the grounds relied on.[424]

In the circumstances, all acts that are prohibited by criminal law can also be censored. One of the most common criminal prohibited content is child sexual abuse material. In Finland, there is a strong online control of child sexual abuse material and therefore there is a separate law against child pornography: The Act on Preventive Measures for Spreading Child Pornography (1068/2006). Thereby the child sexual abuse material is predominantly censored.

However, the other acts prohibited by criminal law, like racism, defamation, libel and intimidation and incitement to terrorism, are not directly predominantly censored. There are no explicit prevention laws in Finland other than The Act on Preventive Measures for Spreading Child Pornography. Hence the other acts prohibited by criminal law can be censored afterwards. The Finnish police have some control over the Internet but much of the work is left to the site administrator: the police trust that administrators will block or filter or remove unlawful content when needed.[425]

One reason why other criminal acts have not actual prevention laws might be that their interpretation is more complicated than child sexual abuse material. Child sexual abuse material is clearly prohibited but for example, defamation can be ambiguous since there are two fundamental human rights against each other: freedom of expression and protection of privacy. Consequently, the censorship is carried out as an ex-post control. One of the major problems with the right to freedom of expression relates to situations where it is used to violate other people's human rights. This raises the question of the limits of freedom of expression: in the Internet era, public expression of opinion is easy, which is why the threshold for expressing abusive or discriminatory opinions is low. Therefore, for example, explicitly racist or threatening material can be censored without violating the right to freedom of expression.[426]

In a similar way, acts prohibited by civil law might never be censored even if they should. In addition, we also have otherwise lawful content which may be blocked, filtered, or removed. Most common is copyright infringements. Intellectual property's content itself is legal but according to Finnish Copyright

---

424 ECtHR Article 10(2). Please see also : Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content. Council of Europe 2015, page 13-14: in general, the main grounds are: the protection of health or morals, including the fight against websites containing child pornography or illegal online gambling websites, the protection of national security, territorial integrity or public safety, including counter-terrorism, the protection of intellectual property rights and the protection from defamation and unlawful treatment of personal data.

425 Lehtisaari, Teemu: Internet-verkon viranomaisvalvonta ja sensuuri 2010, s. 30.

426 Neuvonen, Riku: Viestintäoikeuden perusteet. Helsinki: Talentum Media 2008, s. 49-51.

Act, if someone wants to publish someone else's work on the Internet, they need to have the assignee's permission. For example, if someone adds someone else's photo without the assignee's permission, the site administrator can remove that content even if the content itself is not unlawful. In fact, copyright infringement can be punished as an offence against copyright (under Criminal Code of Finland 49:1) or as a copyright infringement (under Finnish Copyright Act 56 a). Offense and infringement are distinguished by their degree of harm. Copyright infringement occurs, for example, when a song or movie is made available to others on the Internet through a peer-to-peer network without the permission of the assignee. Hence, the acts prohibited by civil law and also by criminal law, often requires that someone inform the site administrator or police about unlawful content. In the case of a complainant offence, it is up to the individual to enforce their rights.[427] According to Finnish Copyright Act Section 60b the assignees have the right to bring an action against the person who gives access to the material allegedly infringed.

3.2. Balancing between censoring and the freedom of expression

Freedom of expression is part of the Constitution Act of Finland and it is one of the fundamental human rights in Finland. Individuals are guaranteed fundamental rights under the constitution, by legislative acts, and in treaties relating to human rights ratified by the Finnish government. Freedom of expression is a fundamental pillar of a democratic society. In practice, freedom of expression means that there is no pre-censorship in Finland. Freedom of expression belongs to everyone, but it also has limits (e.g. hate speech, defamation, and racism). People are not entitled to say whatever they want under freedom of expression. Just like freedom of expression, the fundamental human right is the right to security and peace, the right to private life and the right to religion.

Balancing between censoring and freedom of expression is not easy and it provokes lots of divergent opinions. Members of Finnish Parliament have discussed censorship and its relation to freedom of expression. Jukka Kopra, a member of National Coalition Party (*Kokoomus*), for example, has been worried about the loss of freedom of expression.[428] In addition, there has been a bill amending Criminal Code of Finland since Finnish Parliament wanted to amend the punishable act Chapter 11 Section 10 'Incite against an ethnic group'. This amendment was adopted and will enter into force on the 1 January 2021.

427 Rytinki, Markus: Internetsensuuri Suomessa - Sensuurin aiheet, sensuuriin liittyvät lait ja lakien valvonnan käytäntö 2014, s. 11.

428 Antti Kirkkala : 'Sananvapaus Suomessa on uhattuna.' <https://www.verkkouutiset.fi/sananvapaus-suomessa-on-uhattuna/> accessed 10 June 2020.

According to that section 'any person who deliberately disseminates to the public a message which threatens a group based on race, colour, descent, national or ethnic origin, religion or belief, sexual orientation or disability, social or economic status or political opinion shall be condemned for inciting a fine or imprisonment of up to two years.'

Many members of the Finns Party (*Perussuomalaiset*) have been worried about the loss of freedom because of that amendment to a law. As previously stated, the interpretation of hate speech and defamation might be unclear. Members of Finns Party have stated that this amendment of Criminal Code could drive Finland towards censorship. Finns Party has also stated that according to the Act on the Exercise of Freedom in the Mass Media (460/2003) communication shall not go beyond what is necessary in view of the importance of freedom of expression in a democratic state governed by the rule of law. By prohibiting the expression of any opinion and even factual information, Chapter 11 Section 10 of the Criminal Code severely restricts freedom of expression. They think that the amendment to the Criminal Code will lead to the fact that only sympathetic opinions are publicly accepted in Finland which is contrary to freedom of expression.[429]

Finnish Minister of Justice has responded to the criticism of the Finns Party of restricting freedom of expression by stating that Finland obeys to the European Court of Human Rights' policy that hate speech that may offend individuals or groups does, however, not merit protection of freedom of expression. Furthermore, members of Finnish Coalition Party pointed out that we all have a responsibility for how we exercise this freedom of expression. She also said that according to her own thinking, freedom of expression is abused if it is deliberately used to offend another person or, at worst, to violate the dignity of another person or group of people.[430]

Although Finland is considered a model country for freedom of expression, there is always room for improvement. Riku Neuvonen, a university lecturer in

---

429 LA 30/2019 vp <https://www.eduskunta.fi/FI/vaski/Lakialoite/Sivut/LA_30+2019.aspx> accessed 10 June 2020; PTK 71/2019 vp <https://www.eduskunta.fi/FI/vaski/Puheenvuoro/Sivut/PUH_71+2019+13+36+36.aspx> accessed 10 June 2020; <https://www.eduskunta.fi/FI/vaski/Puheenvuoro/Sivut/PUH_71+2019+13+2+2.aspx> accessed 10 June 2020; <https://www.eduskunta.fi/FI/vaski/PoytakirjaAsiakohta/Sivut/PTK_71+2019+13.aspx> accessed 10 June 2020.

430 PTK 60/2019 vp <https://www.eduskunta.fi/FI/vaski/PoytakirjaAsiakohta/Sivut/PTK_60+2019+2.1.aspx> accessed 10 June 2020.

public law at the University of Tampere, has called attention to the problem that Finnish courts do not necessarily apply the law entirely uniformly. It is possible for a person to be convicted in court of defamation for an act which might not have been seen as reaching the threshold for starting an investigation in another part of the country. This creates an alarming inconsistency in the realisation of freedom of expression in Finland.[431]

3.3. Judicial review

Compliance with the laws must also be enforced. The entities carrying out the monitoring may be added after the above list as follows: courts, police and security police (in Finland National of Investigation). The control of the laws governing censorship on the Internet has not been left solely to the police and the courts. In addition to the police, non-governmental organisations, and potentially individuals, carry out Internet mapping on child sexual abuse material. In copyright matters, interest groups are responsible for enforcing the law, since this is a so-called complainant offense. The most well-known organisations which monitor intellectual property infringements are Teosto ry, Gramex ry and Copyright Information and Anti-Piracy Centre (*Tekijänoikeuden tiedotus- ja valvontakeskus*).[432] All in all, there is a widespread control over the content of the Internet, but there are still certain concentrations. In the cases of child sexual abuse material, the main responsible for monitoring is National Bureau of Investigation which maintains a filter list. In addition, certain Internet intermediaries have a responsibility to act upon their knowledge and to take action in relation to content that is obviously illegal like child abuse material.[433] In intellectual property matters, the Ministry of Education and the Copyright Information and Anti-Piracy Centre play a prominent role. With regard to freedom of expression, one or a few players are more difficult to locate.[434]

With the rise of social media, posting racist messages to forums has increased in recent years. The problem is often the anonymity of these services, which makes it difficult to trace the author. The Ombudsman for Minorities has stated that

---

431 YLE Uutiset: Vihapuhe ja häirintä kaventavat sananvapautta Suomessa – sananvapauden tila on vaihdellut suuresti itsenäisyyden aikana 2019. <https://yle.fi/uutiset/3-10764607> accessed 10 June 2020.

432 Rytinki, Markus: Internetsensuuri Suomessa - Sensuurin aiheet, sensuuriin liittyvät lait ja lakien valvonnan käytäntö 2014, s. 13 ja 15. The Copyright Information and Anti-Piracy Centre is founded by several different Finnish companies like MTV3, Yleisradio Oy, Sanoma Entertainment Oy, the Finnish Musicians' Association etc.

433 Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content. Council of Europe 2015, page 14-16.

434 Rytinki, Markus: Internetsensuuri Suomessa - Sensuurin aiheet, sensuuriin liittyvät lait ja lakien valvonnan käytäntö 2014, s. 14.

the webmaster is primarily responsible for inappropriate messages.[435] However, if this does not agree to delete the messages, you should contact the authorities. In these kinds of cases the police of the author's place of residence may be notified. However, many social media sites may not have active webmasters who constantly monitor the content.[436] On the other hand, the authorities do not have sufficient resources for continuous monitoring, so the situation is quite difficult and challenging. Generally, censorship should always be based on a court order. For example, according to Act on the Exercise of Freedom in the Mass Media (460/2003) Section 18: at the request of a prosecutor, investigator or complaint, the court may order the publisher or program operator, or the operator of a transmitter, server, or other device to suspend the distribution of a published web message if it is clear that its content is punishable. According to Finnish Copyright Act (404/1961) Section 60c: the court can, if conditions are met, order a decision on interruption when dealing with a complaint's claim.

3.4. Case law

Finnish individual named Matti Nikki founded a website named lapsiporno.info (in English child pornography.info) and according to Nikki, the purpose of the site was to deal with the state of Finnish censorship and its problems and to proof that child pornography censorship in Finland was not working properly. However, the website was censored since the National Bureau of Investigation included it on its filter list. In the background here is the Act on Preventive Measures for Spreading Child Pornography which came into force in 2006. The Act on Preventive Measures for Spreading Child Pornography is applied in such a way that the National Bureau of Investigation maintains a secret list of websites that are considered to contain child pornography. Enabling filtering is optional for ISPs, but the Ministry of Communications has indicated that filtering can be made mandatory if needed. To find out what is on the filter list, Nikki wrote a program that went through 100,000 adult entertainment sites. Of these, 785 had been listed by the National Bureau of Investigation, of which only a small proportion were child pornography. In order to substantiate his claim, Nikki published the list on his website. Administrative court of Helsinki did not comment on whether Nikki's website was child pornography or not. However, court stated that Nikki's website could not be listed in the National Bureau of

435 According to the Ombudsman for Minorities, companies maintaining forums must react to the inappropriate content at their site and those companies cannot outsource the responsibility to the volunteer moderators. Please see Nettirasistit halutaan kuriin - lakimuutoksia voi tulla. Uusi Suomi 2008.

436 In Finland hosting providers who have knowledge of illegal content may be expected to remove it voluntarily without judicial authority. Please see also Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content. Council of Europe 2015, page 4.

Investigation's filter list because the Act on Preventive Measures for Spreading Child Pornography only applies to foreign sites, not to Finnish sites.[437] Matti Nikki -case was interesting because Finnish Police was blocking his website but the court stated that the law had been misinterpreted by the police and there was no reason to censor his website.

In the following case, the author's copyright and freedom of expression were facing each other's. Finnish individual Matti Nikki founded the 'Save the Paedophiles' website which was mimicking the well-known 'Save the Children' movement. In the opinion of the Court of Appeal, freedom of expression alone cannot allow copyright infringement.[438] The Court of Appeal stated that while the court order meant restricting Nikki's freedom of expression, protecting the copyrights of the 'Save the Children' movement is more important.

In another case, the current chairperson of the Finns Party *(Perussuomalaiset)* Jussi Halla-aho had published an article on his Internet site containing statements defamatory of Islam and Somalis in 2008. The prosecutor demanded a penalty for incitement against ethnic groups and that he should remove his writings. The Supreme Court of Finland imposed a fine on him and ordered him to remove his writings.[439]

Censorship and the limits of freedom of expression are under evaluation also in one noteworthy, so far inconclusive case. The former chairperson of the Finnish Christian Democrats (*Kristillisdemokraatit*), Päivi Räsänen, is under investigation because of a pamphlet she published on Twitter in 2004 about the gender-neutral marriage: in her view, the Bible entails an unequivocal negative attitude towards homosexuality. The writings have given rise to the question whether Räsänen made herself guilty of ethnic agitation or if these views fit within the limits of freedom of expression. The preliminary investigators argued that if some of the views in the Bible were to be considered as incitement against an ethnic group offence, the dissemination of making available of the Bible would also in principle be punishable as an offense incitement against an ethnic group. Regardless, the Prosecutor General decided to open an investigation, which is still ongoing. According to Räsänen, the greater problem than a fine or imprisonment would be a potential censure requirement: an order to remove social media updates or a ban on writing. She thinks that her punishment would open a passage that would lead to publication bans and modern bonfire of

437 Helsingin hallinto-oikeus 2.5.2011 päätös 11/0403/3 <http://lapsiporno.info/files/Hallintooikeuden%20ratkaisu%202011.pdf> accessed 10 June 2020.
438 Helsingin hovioikeus 15.4.2011.
439 Supreme Court of Finland, KKO 2012:58, 8 June 2012.

books. According to Räsänen, a mere police investigation jeopardises freedom of expression by acting as a deterrent.[440]

Legislation in Finland complies with the requirements which have been set out in the European Court of Human Rights' case law. For example, in the case KKO 2012:58, the district court stated that in interpreting the scope of freedom of expression and its limitations, not only the purpose of the national provisions but also the interpretation of the restriction of Freedom of Expression in the case law of the European Court of Human Rights had to be taken into account. In its numerous judgments, the ECtHR had assessed the protection of Freedom of Expression in Article 10 of the ECtHR in cases where appellants had been convicted in a member state of statements considered to have exceeded the limits of freedom of expression. The district court continued that political opinions were at the heart of freedom of expression and had the strongest protection of freedom of expression. The European Court of Human Rights had repeatedly stated in its reasoning that Article 10 (2) of the ECtHR did not provide much scope for restricting freedom of expression in political speeches or matters of general interest.

According to the European Court of Human Rights, political speech could not be restricted without compelling reasons. On the other hand, the ECtHR had emphasised the importance of tolerance and equality between people as the cornerstones of democracy in its decisions on political statements, and thus on the core issues of freedom of expression. Therefore, according to the reasoning of the court, it may have been necessary to impose sanctions or take preventive measures when statements that incited, created, promoted, defended or attempted to justify hatred based on intolerance, including religious intolerance. The penalties and measures had to be proportionate to the objectives pursued. Hate speech that could offend individuals or groups of people did not deserve the protection of Article 10.

[440] YLE: Päivi Räsäsen krijoituksesta aloitetaan esitutkinta – Epäillään kiihottamisesta kansanryhmää vastaan <https://yle.fi/uutiset/3-11050903> Accessed 10 June 2020; Iltalehti: Päivi Räsänen: Poliisi kuulusteli lähes neljä tuntia 'kristillisen uskon käsitteistä' <https://www.iltalehti.fi/politiikka/a/8fdc58bc-7770-43c3-bc35-402246f0ea68> accessed 10 June 2020.

4. To which extent is the issue of blocking and taking down Internet content self-regulated by the private sector in your country?

4.1. Self-regulation and moderating

Self-regulation refers to the regulation of an issue prepared outside of the official legal system. As it is typically drafted by the actors it concerns themselves, it is often more pragmatic than legislation. Moderating is the most used method of self-regulation on Internet platforms. Moderating practices everywhere in the world are generally based on each country's national legislation, websites' self-regulated rules and on the general rule of conduct of the relevant environment.[441]

In Finland, the legislative basis for moderating consists of preventing crimes such as ethnic agitation, defamation, and menace.[442] Each websites' self-regulated rules are usually expressed in their terms of use. Some categories of actors, such as online magazines', are also affected by non-binding recommendations and rules. This topic will be discussed in more detail in section 4.2. What the general rule of conduct means in each website, depends on users, websites' atmosphere and the picture websites want to maintain or strive for.[443]

Firstly, self-regulated safeguards will be discussed in section 4.2, followed by a discussion on the models used to moderate in section 4.3 and the possible grievance redressal mechanisms in section 4.4. After that, concluding remarks shall be provided on the question 'to which extent is the issue of blocking and taking down Internet content self-regulated by the private sector in Finland?'

Before going into details on this question, it is necessary to set the background. The question about blocking and taking down public content arose to the surface properly around the 2010's. In December 2010, the first fine was issued for a threat made on Facebook.[444] In the year 2011, as conclusion from the terroristic act that happened in Norway, The Criminal Code of Finland went through a comprehensive reform and the expressions 'makes available to the public' and 'keeps available for the public' was added as techniques to the section

441 Paula Haara, Reetta Pöyhtäri and Pentti Raittila, *Vihapuhe sananvapautta kaventamassa* (Tampere University Press 2013).

442 S 25(7), s 24(9) and s 11(10) of the Criminal Code of Finland.

443 Paula Haara, Reetta Pöyhtäri and Pentti Raittila, *Vihapuhe sananvapautta kaventamassa* (Tampere University Press 2013).

444 Jussi Niiranen, 'Astrid Thorsin uhkaajalle 640 euron sakot' *Iltasanomat* (Tampere, 8 December 2010) <https://www.is.fi/kotimaa/art-2000000362004.html> accessed 1 March 2020.

10 of ethnic agitation.[445] This enlarged the liability of social media platforms of the content that the public created on their websites.[446]

In Finland the Council of Mass Media enlarged their Guidelines for Journalists with Annex that concerned media that the public has generated.[447] Many tabloids changed their moderating from subsequent to advanced moderating during Spring 2012.[448] Ethnic agitation is one of the legal bases to delete and block content anywhere. Since 2011, this section has caused variation of opinions whether this also concerns network administrators and their liability for public content published on their websites.[449]

4.2. Self-regulated safeguards

How companies in Finland self-regulate the blocking and taking down of content on their websites depends on the existence of self-regulating committees in their sector or branch, and on each companies' values and evaluations on how harmful the public content is seen for the business. No extensive regulations exists about public content on social media in particular, but the Information Society Code of Finland defines the information services that can be held liable for their public content.[450]

Some of the new outlet media have agreed to be bound by Council for Mass Media's (CMM) Guidelines for Journalists, which have been in force since year 2014. The Guidelines include an Annex called 'Material generated by the public on a media website'. This Annex binds several online magazines, where online discussion is lively in Finland. Annex includes the duty for the editorial office to monitor their own websites and to prevent users' publications which violate privacy and human dignity (i.e. violation of human dignity that incites violence or stirs up hatred towards an individual or group). Also, the editorial office has a duty to delete those publications as soon they become aware of it and to clearly separate forums reserved to the public and editorial content. Specially, online forums designed for children must be supervised carefully. The supervision must include a way to the users to inform editorial offices of privacy and human

445 Ethnic agitation (Amendment of the Criminal Code) Order 2011, SI 511/2011.

446 Explanatory Notes to the Additional Protocol to the Convention on Cybercrime of the Council of Europe on the Criminalization of Racist and Xenophobic Offenses Through Information Systems and the Law on the Provision of Criminal Law and Information Society Services 2010, para 15.

447 Council for Mass Media, Annex: Guidelines for Journalists (1 October 2011) <https://www.jsn.fi/en/guidelines_for_journalists/> accessed 13 February 2020.

448 Paula Haara, Reetta Pöyhtäri and Pentti Raittila, *Vihapuhe sananvapautta kaventamassa* (Tampere University Press 2013).

449 Riku Neuvonen (ed), *Vihapuhe Suomessa* (Edita Publishing Oy 2015).

450 Information Society Code of Finland, s 22(184).

dignity violating content.[451] CMM has given many decisions about online discussions' appropriateness that takes place on Internet magazines' comment sections (4882/SL/12, 5711/SL/15, 5372/SL/13, 5045/AL/12, etc).

The Council of Ethics in Advertising (CEA) has issued principles on marketing that commercial companies must follow. This also applies to the private sector actors when they publish advertisements via Facebook, YouTube or other major platforms.

Additionally, each Finnish private sector company has its own internal guidelines on blocking and taking down the user content. The guidelines are usually confidential, but each company has their own terms of use for users, where major outlines for appropriate user content can be drawn from. Main safeguard model is to moderate user content. Companies either moderate all the content before publishing them or moderate them afterwards. Companies can choose which moderating technique they use.

4.3. Models

The models each company chooses, are based on what the platform wants to protect: their reputation or freedom of expression. Online magazines, for instance, generally need to take into account how the public's comments affect their appearance. Consequently, most such information services review all comments before publishing them. This means that the available forums to use one's freedom of expression's are limited, and the approved comments might paint a false or simple picture of the public's opinion. On the other hand, it has been said that if your comment is blocked or taken down, there is always a platform or forum where you can find like-minded people to express your unmoderated opinion.

A variety of different tools can be employed for the purposes of self-regulation. Some examples include the moderating and filtering of content prior to publishing, informing users that the forum has no responsibility for the content uploaded on it, and reserving the right to remove content and/or users from the forum, sometimes without prior notification. These types of tools are used in most online discussion forums and websites. Some online discussions use user valuation judgements to maintain certain discussion quality.[452] Users can give a thumbs down or up and if a comment gets a certain number of thumbs down, it is either hidden as in anonymous online discussion forum Jodel or gets a reputation as a 'bad comment' as in discussion websites Reddit and Ylilauta.

451 CMM (n 43).

452 Paula Haara, Reetta Pöyhtäri and Pentti Raittila, *Vihapuhe sananvapautta kaventamassa* (Tampere University Press 2013).

Editorials can also give their approval for comments for example by giving them stars. This is the situation in regional paper Helsingin Sanomat. If a comment is valued as good and informative, it is shown higher up in the comment section.

Some information services attempt to reduce the need for moderating by setting conditions (such as creating a user account) for their users to comment or publish on their websites. The strategy can be effective, as many users who upload unlawful or disturbing user content usually want to stay anonymous.[453] The Finnish discussion website Hommaforum attempts to prevent disturbing content by publishing banned users' names on their 'wall of shame'. This practice aims to create public disapproval which might prevent the users from publishing such content again.[454] Most websites put users under special supervision if they constantly upload disturbing and unlawful content. If the harassment does not stop after the moderator has notified the user about website's rules, the user will usually be banned from the website for a certain time period.[455]

Moderators' identity also defines the model information services use. Some use volunteer moderators, which usually are known as decent and active commentators. Internet magazines usually hire professional moderators to moderate their user content. These professional moderators moderate according to the guidelines the website has given to them. For example, such regional papers as Ilta-Sanomat, Helsingin Sanomat and Kainuun Sanomat uses a moderating company STT.

All things considered, there is no common model that all private sector companies use in moderating their user content. The used model depends greatly on the wanted outcome. Helsingin Sanomat, Aamulehti and other major online magazines strive for maintaining a good reputation and in order to do that, they pre-moderate all their user comments before publishing them on comment sections.[456] One feature is still joint for all the companies: they do not give user notification before deleting content or blocking the user. The situation can be changed afterwards if the user complains to the network administrator.

---

453 Paula Haara, Reetta Pöyhtäri and Pentti Raittila, *Vihapuhe sananvapautta kaventamassa* (Tampere University Press 2013) and Reetta Pöyhtäri, 'Tietoverkkojen sääntelyn erityiskysymykset vihapuheen osalta' in Riku Neuvonen (ed), *Vihapuhe Suomessa* (Edita Publishing 2015) ch 7, 89–116.

454 Upkeep of Hommaforum, 'Codex Hommaforum' *Hommaforum* (25 May 2018) ch 8 <https://cms.hommaforum.org/index.php/homman-nimi/saannot> accessed 29 February 2020.

455 Paula Haara, Reetta Pöyhtäri and Pentti Raittila, *Vihapuhe sananvapautta kaventamassa* (Tampere University Press 2013).

456 Riku Neuvonen (ed), *Vihapuhe Suomessa* (Edita Publishing Oy 2015).

4.4. Grievance redressal mechanism

There are information services' own redressal mechanisms and then there are few committees that offer redressal mechanisms. In Finnish discussion website Suomi24, grievance redressal mechanism is carried out by giving the users an opportunity to notify the network administrators or to point out to the other users that their behaviour is not according to the website's rules. Usually the discussion websites have more detailed terms of use than online magazines.[457] Both Hommaforum's and Suomi24's users can make notices of inappropriate messages and these notices usually are the basis for subsequent moderation. Moderators can join the discussion in order to remind users about the rules or to calm down the discussion. If moderators have deleted a user's comments, they can explain why it was deleted or why this comment was not allowed in the comment section.

CMM has a grievance redressal mechanism and they give non-binding resolutions to their members. These resolutions cannot be appealed. Also, CEA issues nonbinding statements on whether an advertisement is ethically acceptable (according to ICC Code of Advertising and Marketing Communication Practice) from consumers' requests. For example, in MEN 38/2019 CEA decided that an advertisement uploaded on Facebook by a bar was discriminatory.

In some discussion websites, users may appeal or otherwise contact the network administrator if they feel that their content has been deleted on a wrongful basis. This is the case for example in Jodel and Hommaforum.[458]

4.5. Conclusion

Private sector forums and websites can decide independently 1) if they take the responsibility or not on the content users upload, comment or otherwise publish; 2) if they are bound by certain councils' recommendations; and 3) choosing the tools and/or methods to block or filter the public content on their websites.

Each information service informs their users about their policies on blocking and deleting content in their terms of use. From the point of view of the freedom of expression, moderating can be potentially problematic if it results a skewed

457 Paula Haara, Reetta Pöyhtäri and Pentti Raittila, *Vihapuhe sananvapautta kaventamassa* (Tampere University Press 2013).

458 Jodel, 'Terms of Use', Jodel (March 2019) pt 14 <https://jodel.com/terms/> Accessed 29 February 2020 and Upkeep of Hommaforum, 'Codex Hommaforum' Hommaforum (25 May 2018) ch 9 <https://cms.hommaforum.org/index.php/homman-nimi/saannot > accessed 29 February 2020.

picture of the public opinion, for instance through the categorical removal of certain opinions or groups from the discussion.

Freedom of Expression does offer protection to hate speech. The line between unlawful and lawful user-created content can sometimes be hard to draw; how this is done is primarily in the hands of each websites' moderators. This easily results in discrepancies in the existing practices, and there is typically no certainty of whether the comments which have been approved or disapproved into the comment section are truly lawful. The practices are purely based on each information service's own rules. Especially online newspapers often refrain from publishing even lawful comments if they are seen as potentially harmful for the newspaper's reputation. This can be problematic in the view of freedom of expression, especially if there are few alternative forums in which said opinions could be expressed.

Despite the problems, it is still better for Freedom of Expression that information services themselves have the power to decide which content they wish to approve, if the other option is to centralise the process and give this right to the state.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

5.1. The General Data Protection Regulation and the right to erasure

The General Data Protection Regulation (the 'GDPR', EU 679/2016) became applicable on 25 May 2018 and replaced the old Data Protection Directive (95/46/EC)[459]. The GDPR is directly applicable in all EU Member States, thus also in Finland. The main purpose of the reform is to further ensure the protection of personal data and to improve the efficient functioning of the internal market. This is achieved by creating a single data protection framework for the EU internal market with as little national variation as possible.[460] The fundamental rights have also formed an essential part of the legislative framework. This has also reflected into the interpretation of the personal data protection provisions.[461] The free movement of information still has a central role but the balance between personal data protection and free movement of

459 Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

460 Päivi Korpisaari. Henkilötietojen ja yksityiselämän suoja vuonna 2018 - Katsaus sääntelyyn ja ratkaisukäytäntöön. 27.

461 Joined Cases C-92/09, Schecke and C-93/09, Eifert, ECLI:EU:C:2010:662.

information has shifted.[462] The scope of the Chapter 5 in this research paper examines the Right to be Forgotten in Finland with regards to Internet censorship.

The Right to Erasure appears in Recitals 65 and 66 and in Article 17 of GDPR. The Right to Erasure is also known as the 'Right to be Forgotten' or the 'Right to Delete'. It states, 'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay' if any of the conditions apply.[463] According to Article 12 undue delay is one month. It should be noted that the right to erasure is not as such a new right provided by the GDPR since it was already present in the superseded Data Protection Directive. The Right to be Forgotten concerns on-demand erasure of all records of the information and empower the data subject to control the usage of personal data.[464] This means that the service provider must comply with deletion requests unless the information is required for exercising the right of freedom of expression and information, for compliance with a legal obligation, for reasons of public interest or for the establishment, exercise or defence of legal claims.[465]

The Constitution of Finland provides that 'Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.'[466] The Data Protection Act, in force as of 1 January 2019, complements and specifies the provisions of the GDPR serving as a general personal data protection law in Finland. The Data Protection Act repealed the Personal Data Act of 1999, which had already, in addition to several other legal acts, provided a high level of data protection in Finland also including the Right to be Forgotten. The Data Protection Act provides an exclusion to Article 17 of GDPR in order to safeguard Freedom of

462 Anu Talus. Tietosuojasääntelyn Eurooppalaistuminen - It is an evolution, not a revolution. Defensor Legis N:o 2/2019. 216.

463 GDPR, Article17(1)(a). the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; Article17(1)(b). The data subject withdraws consent on which the processing is based; to Article 21.1 and 21.2. The data subject exercised his or her Right to object to processing of his or her personal data; Article17(1)(d). The personal data have been unlawfully processed; Article17(1)(e). The erasure is compliant with a legal obligation; Article17(1)(f) which refers to Article8.1. The personal data have been collected in relation to the offer of information society services to a minor.

464 Subhadeep Sarkar, Jean-Pierre Banatre, Louis Rilling and Christine Morin. Towards Enforcement of the EU GDPR: Enabling Data Erasure. IEEE Conference Publications on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics. Halifax. Canada. 2018. 222-229.

465 GDPR, Article 17(3)(a)-(e).

466 Perustuslaki 11.6.1999/731, Chapter 2, Section 10.

Expression and information for the purposes of the processing of personal data solely for journalistic purposes or for academic, artistic or literary purposes.[467]

5.2. Specific Legislation

The GDPR contains, in certain respects, a national margin of discretion. As a result, there is an exceptional amount of changes needed in order to bring the national legislation in line with the GDPR.[468] Working group set by the Ministry of Justice identified over 800 specific legislation in for legislative work.[469] The report highlighted concerns related to the implementation of Article 9 on public interest. However, it did not raise any special considerations related to reform needs arising from the Right to be Forgotten.[470] In many respects, these changes are technical, and the key to their implementation has been the reinforcement of the content and entry into force of the new national Data Protection Act. Although the Data Protection Act has been adopted and ratified, the reform of other legislation is still in its early stages. Most of the specific legislation deals with how authorities process personal data. They provide either derogation from the general legislation in order to more closely specify how the personal data is to be processed or impose particular provisions on how to process personal data in a specified field.[471]

Finland follows a wide publicity principle.[472] According to the GDPR Recital 154, it is in the public interest that the principle of publicity and the protection of personal data can be reconciled within a national margin of discretion. The principle of publicity is laid down in the Constitution of Finland (731/1999) Section 12 on Freedom of Expression and Right of Access to Information. Only the public sector documents are regulated. The publicity legislation and its reconciliation with the protection of personal data have always received special attention in Finland.[473]

---

467 Tietosuojalaki 5.12.2018/1050, Section 27.

468 Jukka Lång and Tuomas Haavisto. Mitä muutoksia uusi kansallinen Tietosuojalaki tuo käytännössä? Edilex 2019/2. <https://www.edilex.fi/artikkelit/19271.pdf> Accessed 15 January 2020.

469 EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) loppumietintö. Oikeusministeriö. Mietintöjä ja lausuntoja. 8/2018. Helsinki. 2018.

470 Ibid., and Olli Pitkänen. (toim.) Tietosuojasäädösten muutostarve. Valtioneuvoston selvitys- ja tutkimustoiminta. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017.

471 EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) loppumietintö. Oikeusministeriö. Mietintöjä ja lausuntoja. 8/2018. Helsinki. 2018. 28-32.

472 Ibid., 20.

473 Tuomas I. Lehtonen. Tietosuojalainsäädäntö ja julkisuusperiaate törmäävät vastakkain. Lakimiesuutiset. 18.2.2020. <https://lakimiesuutiset.fi/tietosuojalainsaadanto-ja-julkisuusperiaate-tormaavat-vastakkain/> Accessed 21 February 2020.

5.3. Jurisprudence and decisions of competent authorities

The Data Protection Ombudsman (the 'DPO) is the Supervisory Authority in Finland assessing the complaints regarding a search engine provider who has refused to delete a specified search result pursuant to Article 17. At the time of writing all rulings on the right to be forgotten within the scope of this research paper, Internet censorship, are based on the Data Protection Directive and thus the national Personal Data Act. The DPO has taken into account national law, the Court of Justice of the European Union (the 'CJEU') case law, the European Court of Human Rights (the 'ECtHR') case law and the WP29 guidelines[474] in particular when making a decision regarding the right to be forgotten. The WP29 guidelines provide 13 common principles to be taken into account when reaching a decision. The principles are as follows:

1. Does the result relate to a natural person i.e. an individual? Does the search result come up against a search on the data subject's name?; 2. Does the subject play a role in public life? Is the data subject a public figure?; 3. Is the data subject a minor?; 4. Is the data accurate?; 5. Is the data relevant and not excessive? Does the data relate to the working life of the data subject? Does the search result link to information which allegedly constitutes hate speech/slander/liberal or similar offences in the area of expression against the complaint? Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?; 6. Is the information sensitive within the meaning of Article 8 of the Directive 95/46/EC?; 7. Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?; 8. It the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the date subject?; 9. Does the search result link to information that puts the data subject at risk?; 10. In what context was the information published? Was the content voluntarily made public by the data subject? Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?; 11. Was the original content published in the context of journalistic purposes?; 12. Does the publisher of the data have a legal power or legal obligation to make the personal data publicly available?; and 13. Does the data relate to a criminal offence? As is made clear by the number of factors to be weighed in, decision making in each individual case requires a careful balancing act.

474 European Data Protection Board. GDPR: Guidelines, Recommendations, Best Practices <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en> accessed 21 February 2020.

Out of 48 cases, the DPO gave 12 rulings to delete all Google search results that led to websites containing personal information of the data subject.[475] In addition, two rulings provide that only some of the search results were to be deleted, not all.[476] In most of the cases, three legal questions arise based on the principles provided in the WP29 guidelines.

Firstly, does the data subject play a role in public life and is the data subject a public figure?[477] A general rule provides that public access to information offers protection against improper public or professional conduct, an interest which needs to be weighed in in the decision. Public roles and activities could include, for instance, political activity,[478] business activities[479] or criminal offences.[480] A mere participation in an occasional online chat does not mean that a person would be in such a position.[481] It is also not the case that, for instance, a criminal offender does not enjoy any protection of privacy at all. A part of the personal data of the data subject remains covered by the protection of private life or by the fundamental right to privacy, notwithstanding the criminal offence and the penalty imposed for it.[482]

Secondly, is the information of the data subject currently irrelevant, inaccurate, incomplete, or outdated for the purpose of the processing of personal data?[483] Personal data can be roughly classified into undisputed facts and subjective opinions or views about a person. If objectively observable, factual errors in the information in question give an inaccurate, incomplete, or misleading image of

475 Docket no 637/533/2018, 28.9.2018; Docket no 2524/533/2015, 27.8.2018; Docket no 85/533/2015, 25.9.2018; Docket no 2328/533/2016, 12.9.2018; Docket no 1504/533/2017, 7.9.2018; Docket no 1967/533/2017, 27.8.2018; Docket no 1973/533/2014, 31.7.2018; Docket no 3668/533/2017, 12.7.2018; Docket no 2009/533/2014, 21.12.2016; Docket no 3190/533/2014, 19.2.2016; Docket no 2024/533/2014, 5.1.2016; Docket no 1374/533/2015, 3.12.2015.

476 Docket no 1379/533/2018, 27.9.2018; Docket no 866/533/2016, 13.7.2018.

477 See Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González EU:C:2014:317, paragraphs 97, 99-100.

478 Docket no 1504/533/2017, 7.9.2018: Candidate in Parliamentary elections.

479 Docket no 1967/533/2017, 27.8.2018: A sales representative was not, according to the public register, in a position that would acquire being responsible of company's affairs, f.ex. signatory rights on behalf of the company. page3.; Docket no 2328/533/2016, 12.9.2018: In analogy with the former arguments, the public relations manager was not, according to the public register, one of company's responsible persons. 3.

480 Docket no 3668/533/2017, 12.7.2018: Criminal act and being convicted of it gives a person a public position in society and puts him in the so-called media exposure for that act. The premise is that the perpetrator of the crime cannot, after the act, have a reasonable presumption as to the extent of his or her data protection as for the offence with an innocent person. 3; Also see *Sidabras and DŽiautas v. Lithuania* Appl. nos. 55480/00 and 59330/00 (ECtHR 27.7.2004), paragraph 49; *Axel Springer Ag v. Germany* Appl. no. 39954/08 (ECtHR 7.2.2012) paragraph 83.

481 Docket no 1973/533/2014, 31.7.2018, 3.

482 Docket no 866/533/2016, 13.7.2018, 3.

483 Former Personal Data Act, 523/1999, Section 9. See also Case C-131/12, paragraph 94.

a person, the order for the erasure is more likely to be given[484]. The interest of the public availability of information is carefully considered, however.[485] Cases dealing with data subject's criminal history as a search result are dealt with analogically with the public availability of criminal records.

Thirdly, should the order be given by the DPO to correct (i.e. delete) the information? Only one case has proceeded to the Supreme Administrative Court.[486] At the time of writing no conclusion can be drawn on possible changes to principles and doctrines due to the GDPR in terms of rulings of the DPO.

The Finnish Supreme Administrative Court considered a data subject's Right to be Forgotten for the first time in its judgment rendered on 17 August 2018. The case concerned removing Google search results that led to websites containing data subject's criminal history, in addition to health and mental data. The Court held that the public interest in receiving information about the data subject did not rule out his Right to Privacy and Personal Data. As a result, search results could be ordered to be deleted. The Court also held that Freedom of Expression cannot prevail over the Right to Privacy of the data subject. The judgement is in analogy with the CJEU Google Spain case providing that the rights of a data subject override both the rights of the search engine operator and the interests of the general public in accessing information from searching a data subject's name. The Court held that a fair balance needs to be found between these rights and interests, which can depend on the nature of the information in question.[487] Furthermore, the interest of the general public may vary according to the data subject's role in public life.[488]

As mentioned earlier, the Data Protection Act provides exceptions in order to safeguard journalism in addition to academic, artistic and literary expression. The activity of the website publisher may be for journalistic purposes, even if the search engine results for the activity are not.[489] However, the CJEU rulings

484 Docket no 85/533/2015, 25.9.2018: Error in facts: The data subject was not convicted of aggravated fraud.

485 Docket no 3668/533/2017, 12.7.2018: 20-30-year-old criminal history is not available in public criminal records and is not relevant to the public interest.; Docket no 1967/533/2017, 27.8.2018 and Docket no 1504/533/2017, 7.9.2018: Time period of two consecutive parliamentary terms in terms of political opinions is of public interest.

486 Supreme Administrative Court of Finland, KHO 2018:112, 17 August 2018.

487 See Case C-131/12, paragraph 81.

488 KHO 2018:112.

489 HE 9/2018 vp, Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

provide that maintaining a search engine is not the same as processing personal data for journalistic purposes.[490]

A preliminary ruling by the CJEU and the ECtHR in case *Satakunnan Matkapörssi Oy and Satamedia Oy v. Finland* reviewed the notion of journalistic purpose, the right of dissemination of personal data acquired through access to public documents and balance of Freedom of Expression and Right to Privacy.[491] The ECtHR held that 'the general transparency of the Finnish taxation system does not mean that the impugned publication itself contributed to a debate of public interest'.[492] A Right of Access to public documents does not by itself justify the dissemination of these documents or the data they contain.[493] The Court provided that the restrictions were prescribed by law and pursued the legitimate aim of protecting the right to privacy of taxpayers, there is no journalism exception for massive exposure of personal taxation data. The fact that the data was already public did not remove the protection of Article 8 of the European Convention on Human Rights. However, the Court did not clearly establish what is the acceptable limit to which extent the taxation data could be published in terms of data journalism in Finland.

6. How does your country regulate the liability of Internet intermediaries?

Finnish legislation for the liability of Internet intermediaries is based on the implementation of the EU Information society directive. In general, Internet intermediaries do not have an obligation to actively monitor, or moderate content on their platform or implement any tools for the users to report potentially illegal content - as required in the European Union's 'Directive on electronic commerce' Article 15.[494] However, there are few situations where intermediaries are required to remove or block access to illegal content.

490 Case C-131/12, paragraph 58 and by analogy, Case C-324/09 L'Oréal and Others EU:C:2011:474, paragraphs 62-63.

491 Case C-73/07, Satakunnan Markkinapörssi and Satamedia, ECLI:EU:C:2008:727, Grand Chamber judgement on 16 December 2008; ECtHR, Case *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, App no 931/13, Grand Chamber judgment on 27 June 2017.

492 ibid, paragraph 174.

493 ibid, paragraph 175.

494 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

6.1. Terminology

'Internet intermediary' is a broad term for companies which facilitate the use of the Internet. Examples of Internet intermediaries include e.g. caching and hosting providers and social media services.

'Caching' refers to the automatic, intermediate, and temporary storage of information in a communications network performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service. 'Hosting service' provides storage of information to a recipient of the communications network service.

6.2. Hosting services

Finnish Information Society Code states that a hosting service is not liable for the content if it acts expeditiously to disable access to the information stored upon:

- obtaining knowledge of a court order concerning it or if it concerns violation of copyright or neighbouring right upon obtaining the notification; or
- otherwise obtaining actual knowledge of the fact that the stored information is clearly contrary to:
- Section 10 or 10(a) of Chapter 11 (Ethnic agitation or Aggravated ethnic agitation); or
- Section 18 or 18(a) of Chapter 17 (Distribution of a sexually offensive picture or Aggravated distribution of a sexually offensive picture depicting a child) of the Criminal Code.[495]

In addition, according to Act on the Exercise of Freedom of Expression in Mass Media[496] a court may order Internet intermediary to cease the distribution of a published network message, if it is evident that providing the content to the public is a criminal offence. This covers for instance offences against privacy, public peace and personal reputation such as Dissemination of information violating personal privacy[497] and Defamation[498] described in the Finnish criminal code.

In other words, hosting providers are not liable for the user generated content hosted on their platforms unless they do not react, and remove or block access

495 Laki sähköisen viestinnän palveluista (917/2014) 184 §, Rikoslaki 11. luku 10 §, Rikoslaki 17. luku 18 §.
496 Laki sananvapauden käyttämisestä joukkoviestinnässä (460/2003) 18 §.
497 Rikoslaki (39/1889) 24. luku 8 §.
498 Rikoslaki (39/1889) 24. luku 9 §.

to content based on court orders or IPR takedown requests, or if they do not remove hate speech content or sexually offensive material they have actual knowledge of.[499]

6.3. Caching services

Caching service providers are obligated to remove cached content that has been removed from the original source, or when a court or an administrative authority has ordered such removal or disablement.[500]

6.4. Safeguards

Hosting services have the freedom to moderate user generated content based on their own terms of service. Moderation is voluntary, but a common practice in biggest Finnish social networking services and in user commenting sections of mass media publications.

There are several safeguards for the service and content providers in order to avoid government censorship. Court order to disable access to information can be made by a public prosecutor, a person in charge of criminal investigation or alternatively by a party whose right the matter concerns. The court shall process the request urgently and the application cannot be processed without the service provider (i.e. Internet intermediary) and the content provider to be consulted - except if the consultation cannot be arranged as quickly as the matter requires.[501]

Content provider must be informed by the court and if the content provider is unknown, the service provider may be ordered to take care of the notification.[502] Order in question will become ineffective unless criminal or civil charges are raised within the next three months. The court may extend this time limit by a maximum of additional three months in case the original time limit is not enough for instance in order to find out the identity of the content provider.[503]

Both the service provider and the content provider have the right to apply for reversal of the order within 14 days of the date when the applicant was notified of the order.[504] If the service provider has blocked access to the data, it must notify the content provider stating the reason for prevention and information on the right to be heard at a court hearing. The notification in question must be

---

499 According to government proposal for the Information society code, 'actual knowledge' means that the service provider knows the content exists, it is location and that the content in question is clearly illegal, HE 194/2001.

500 Laki sähköisen viestinnän palveluista (917/2014) 183 §.

501 Laki sähköisen viestinnän palveluista (917/2014), 185 § 1. mom.

502 Laki sähköisen viestinnän palveluista (917/2014), 185 § 2. mom.

503 Laki sähköisen viestinnän palveluista (917/2014), 185 § 3. mom., HE 194/2001.

504 Laki sähköisen viestinnän palveluista (917/2014), 185 § 4. mom.

made in the mother tongue of the content provider, in Finnish or in Swedish.[505] The content provider has the right to bring the matter to the court within 14 days from the receipt of the notification.[506]

Regarding IPR violations, the copyright owner or their legal representative can request a service provider to block access to material infringing upon the copyright. The request must first be presented to the content provider but if the content provider cannot be identified, or if she/he does not remove or block access to material in question, the request may be submitted to service provider (such as a hosting service or other Internet intermediary).[507]

A notification that does not contain required information, is invalid but the service provider must take necessary steps in order to communicate the shortcomings to the notifying party.[508] In addition, service providers are required to notify the content provider of blocking access supplied by her/him with a copy of the copyright notification. If the content provider considers the prevention is groundless, she/he may get the material returned by delivering a plea to the notifying party within 14 days of receiving the notification. A copy of the plea must be delivered to the service provider. The plea must include name and contact information of the content provider, facts and reasons for groundless prevention, itemisation of the material for which prevention is considered groundless and the signature of the content provider.[509]

If the plea meets the requirements and is delivered within the time limit, the service provider must not prevent the material from being returned and kept available unless otherwise agreed between the service provider and the content provider or by an order or decision by a court or by any authority.[510]

A person who gives false information in the copyright notification or in the plea, is liable to compensate for the damage caused.[511]

6.5. Conclusions

Online Freedom of Expression is not heavily regulated in Finland. Internet intermediaries are required to remove clearly illegal content based on court orders, IPR takedown requests or actual knowledge of hate speech or sexually offensive material. Criminal liability for the content that is hosted requires intent,

505 Laki sähköisen viestinnän palveluista (917/2014), 187 § 1. mom.
506 Laki sähköisen viestinnän palveluista (917/2014), 187 § 2. mom.
507 Laki sähköisen viestinnän palveluista (917/2014), 189 § 2. mom.
508 Laki sähköisen viestinnän palveluista (917/2014), 191 §.
509 Laki sähköisen viestinnän palveluista (917/2014), 192 §.
510 Laki sähköisen viestinnän palveluista (917/2014), 193 §.
511 Laki sähköisen viestinnän palveluista (917/2014), 194 §.

but most Finnish platform providers have avoided this. Platforms and forums do not want to host illegal content — they have content guidelines for their users, moderation processes and reporting tools in place which has led to a situation where illegal content is very often noticed and taken down by the service provider when users report it. In that sense the situation seems to be quite ideal: the Finnish discussion on freedom of expression is mostly focused on the potential criminalisation of specific acts by individuals and on the fine tuning definitions of illegal content - not increasing the liabilities of Internet intermediaries.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of Internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1. Finnish governmental planning and overview

In the Finnish parliamentary system, a multiparty government creates a governmental programme for their four-year term that outlines the major pieces of legislation they intend to enact. The current governmental programme lists as one of its objectives to 'address systematic harassment, threats and targeting (author's note: this term will be discussed at length below) that impedes Freedom of Expression, the work of public authorities, research and transmission of information.'[512] There is no other mention of the topics raised in this question in the programme. That does not mean that these issues are not significant topics in the national political discussion, but no immediate domestic legislative action is planned outside of *targeting*.

The EU has taken substantial action in this field and brought these issues into the legislative discussion, as both GDPR and the Right to be Forgotten are concepts originating from the EU. These are, in essence, questions of consumer protection and Finland with a population of five and a half million people is likely to enact substantive change through collective action in the EU than through national legislation, given that the major actors in these fields are international giants such as Google and Facebook.

The major trends that will probably be subject to domestic political discussion in the near future are *targeting* and the future of data economy. Hate speech

[512] Programme of Prime Minister Sanna Marin's Government, 10 December 2019, page 97, <http://urn.fi/URN:ISBN:978-952-287-811-3> accessed 24 February 2020.

related legislation is not a topic covered by this question. As discussed above, the push for legislation in these topics will likely be from either the EU or non-state actors rather than the legislature itself.

7.1.1. Criminalisation of targeting

An important piece of legislation affecting Freedom of Expression and online intermediaries is a bill aiming to criminalise *targeting* (maalittaminen). There is no direct translation for *maalittaminen* as it is a novel term that lacks a clear definition even in Finnish. In colloquial use it refers to several online activities such *dog-piling*, *virtual mobbing* and *doxxing*. In essence *targeting* means subjecting someone to harassment online, usually by encouraging negative attention or engagement. In this report the term *targeting* in cursive is a translation for the Finnish term *maalittaminen*.

The Finnish Government programme lists as one of its objectives to address systematic harassment, threats and *targeting* -- the work of public authorities. Several entities such as the Association of Finnish Lawyers and the Finnish Police Federation are also in favour of the criminalisation of *targeting*[513].

In the context of the proposed law on *targeting* the meaning of the term is quite different than expressed above. The bill aims to criminalise *targeting* (i.e. various forms of harassment targeting) a civil servant or their family members when the harassment may affect or disturb their ability to carry out their official duties. Activities included within the term *targeting* are: harassment, making threats, and making, distributing or otherwise disseminating unfounded claims. In the foreword of the bill one example of *targeting* is 'the use of mass power in social media'. *Targeting* is also differentiated from hate-speech, as it is considered to be 'systematic activity' and not just individual comments or posts. Additionally, during parliamentary discussion, proponents of the bill listed a wide variety of issues from sending a funeral candle or a hand grenade to a police officer's home to a barrage of emails in one's inbox.[514] It is clear that though the newly coined legal term *targeting* and its colloquial equivalent overlap, they are not consistent with one another.

513 Lakialoite LA 33/2019 vp.

514 Comment by Member of parliament Kari Tolvanen. Parliamentary session 27 November 2019. 19.49. Recorded in PTK 71/ 2019 vp. <https://www.eduskunta.fi/FI/vaski/PoytakirjaAsiakohta/Sivut/PTK_71+2019+16.aspx> accessed 10 June 2020.

7.1.2. Who can be held criminally liable for targeting?

Two key aspects of the Bill, as it currently reads, require elaboration: The scope of individuals that can be charged with said crime and the liability of intermediaries.

The Bill states that criminal targeting can be carried out independently, by instigating or by participating in the aforementioned activities. In terms of guaranteeing that the law does not infringe on people's Freedom of Expression, the limits of what constitutes instigation and participation have to be clearly defined. One object of the criminalisation is to secure a safe online presence for civil servants but not to shield them from criticism. Therefore, it should be made clear that the law should not extend liability to actors who for example participate in a dog-pile without clear evidence of malice and an understanding of participating in a coordinated effort to harass. Otherwise activity protected as free speech might lead to criminal liability as *participation in targeting* simply due to simultaneous actions of others.

The Bill also extends the criminal liability to an entity 'that knowing of the purpose of aforementioned means [i.e. harassment of a civil servant] provides a platform for such activity'. This raises the question that could, for example, twitter be held criminally liable in a case of dog-piling? A limiting factor is the requirement that the intermediary has to 'know of the purpose' of the criminal activity. This would probably only be applicable to forums or other platforms that openly tolerate or encourage activity classified as *targeting*, especially if the users of said platform are allowed to act anonymously.

However, imageboards, such as 4chan.org or ylilauta.org, that commonly host discussions that could be within the scope of the bill, are not usually the platforms where the damage or threats actually occur as civil servants probably do not scourge said websites for feedback. Discussions on such imageboards become a form of *targeting* when people participating in or viewing those discussions act on them on more common social platforms (Twitter, Facebook) or in real life. So, a dog-pile that occurs on twitter can have its origin on a completely unrelated platform. It is important that the legislature considers and defines what are the actual liabilities of different platforms that may be involved in different stages of more-or-less coordinated *targeting* activity.

The Bill will go through further stages of drafting and modification so the broad definitions used in the bill will hopefully be defined more strictly. However, criminalisation of *targeting* will likely happen in one form or another, as it enjoys wide support from the government, parts of the opposition as well as several major organisations. It is clear that at least some platforms, most likely

imageboards, will have further liabilities in managing and deleting content. For example, ylilauta.org (the most visited imageboard in Finland) already prohibits posts that are 'illegal or promote illegal activity' or 'intended to harass or threaten others or promote such activity', but given the proposed bill, the scope of 'illegal activity' would definitely become broader.[515]

7.2. Data economy

During Finland's presidency of the Council of the European Union, Finland hosted a conference on data economy where a paper called *Principles for a human-centric, thriving and balanced data economy* was released.[516] The principles are not a binding resolution, rather a framework for future development in data economy. There is a clear shift in the discussion in the data economy field from Silicon Valley start-ups setting the tone in the early 2000's to current intergovernmental action on reining in the excesses and protecting user privacy. Finland is positioning itself as an advocate for digital privacy rights, though this might not translate into further national legislation.

Sitra, the Finnish Innovation Fund, is a politically independent research fund whose one main objective is to research, support and develop tools for Finland as a 'pioneer in sustainable well-being'.[517] Their reports are provided to the parliament as well as published for the public so they have a significant role in setting the agenda for policy discussions in certain fields. One major project currently active at Sitra focuses on creating the foundations for a sustainable data economy.[518] A study in 2019 showed that 42 % of respondents reported that a lack of trust in online actors prohibited them from using some digital services.[519] A study published in early 2020 (currently preliminary results, full report in [520]) details how privacy protections guaranteed by GDPR are not fulfilled by digital actors. The research also noted how websites, games and apps collect and use data of children without the express consent of their parents.[521] There has also

---

515 Säännöt. Ylilauta.org. <https://ylilauta.org/?saannot> accessed 12 February 2020.

516 Principles for a human-centric, thriving and balanced data economy. EU2019.fi. <https://api.hankeikkuna.fi/asiakirjat/2d0f4123-e651-4874-960d-5cc3fac319b6/1f6b3855-fc1d-4ea6-8636-0b8d4a1d6519/RAPORTTI_20191123084411.pdf> accessed 10 June 2020.

517 Sitra: About Us <https://www.sitra.fi/en/themes/about-sitra/#our-work> accessed 10 June 2020.

518 IHAN project: Fair Data Economy <https://www.sitra.fi/en/topics/fair-data-economy/> accessed 28 February 2020.

519 Jaakko Hyry, Kanter TNS Oy. Digitaalisten palveluiden käyttö - Kyselytutkimus neljässä maassa. Kokonaisraportti. Sitra. page 23. <https://media.sitra.fi/2019/01/16140515/digitaaliset-palvelut-kyselytutkimus-neljassa-maassa.pdf> accessed 10 June 2020.

520 Data collected about people is hidden in complex networks. Sitra. <https://www.sitra.fi/en/articles/data-collected-about-people-is-hidden-in-complex-networks/> accessed 10 June 2020.

521 ibid. 24-25, 29.

been public discussion regarding the terms of service of and data collection by digital tools in learning environments.

7.3. Conclusions

When analysing the possible future development of these issues in Finland, the data economy is still a fairly obscure concept. However, it will likely gain more traction in the media through the advocacy of actors such as Sitra. Public awareness will probably lead to policy proposals, but the right instance for action will be the EU. Further legislation related to GDPR might be called for, but Finland has already passed fairly strict GDPR compliant data collection and privacy laws. *Targeting* is a more domestic issue and will be criminalised in one form or another in the near future.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

8.1 The definition of hate speech

The concept of hate crime and hate speech is not specifically defined in the Finnish legislation. According to the Finnish Police University College's report on hate crimes, the term hate crime generally refers to a crime that is made against a person, group, property, institution or their representatives, which is motivated by prejudice or hostility towards the victim's real or perceived ethnic or national origin, religious beliefs or ideology, sexual orientation, gender identity, gender expression or disability.[522] It is important to point out that the definition does not presuppose that the victim actually belongs to one of the reference groups listed above, but that it is sufficient for the offender to have assumed it.[523] A commonly used definition for hate speech is found in the Council of Europe Committee of Ministers Recommendation No. R (97) 20 of the Committee of Ministers to Member States on 'Hate Speech'.[524]

---

522 Jenita Rauta, Poliisin tietoon tullut viharikollisuus Suomessa 2018, <http://urn.fi/URN:NBN:fi-fe2019102935508> (Poliisiammattikorkeakoulun raportteja, Poliisiammattikorkeakoulu 2019) accessed 10 June 2020.

523 Riku Neuvonen, Vihapuhe Suomessa (Edita Publishing Oy 2015) 119.

524 Recommendation No. R (97) 20 Of the Committee Of Ministers To Member States On 'Hate Speech' (adopted by the Committee of Ministers on 30 October 1997, at the 607th meeting of the Minister's Deputies) <https://rm.coe.int/1680505d5b> accessed 24 January 2020: The recommendation defines the term hate speech as follows: '--the term 'hate speech' shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, antisemitism or other

The term hate speech used in general language and public discourse has become a concept that is open to interpretation. Traditionally hate crimes have been connected with the hate motive but there is also found a new form of hate speech where for example journalists and researchers are the subject of hate speech due to their opinions in matters such as immigration or vaccines. If expressions do not fulfil any essential elements of an offence, it may be difficult to intervene. Therefore, this new form of hate speech can cause a muting effect also to public discourse by influencing the work of authorities, scientist and journalists.[525]

Hate speech has many manifestations, which makes it harder to recognise and punish. The same expression can fall under the definition of hate speech in one context yet be acceptable in another. The most identifiable form of hate speech is threat or incitement to commit violence or crime. Slandering or insulting could also be considered as hate speech. In such situations, the distinction between prohibited hate speech and protected freedom of expression becomes more unclear. Nevertheless, freedom of expression enjoys strong protection when it comes to matters of general interest. Contempt and incitement to hatred of certain ethnic groups are incompatible with the values of a democratic society but on the other hand, Freedom of Expression protects also harmful, disturbing, and critical statements if deemed necessary in the light of public discourse. Thus, many cases require weighing up conflicting interests and the solution depends entirely on the details and the context of the case.[526]

8.2 Punishable hate speech

As there is no legal definition for hate speech in the Finnish legal system, the number of hate speech cases has to be inferred from the hate crime statistics. According to the reporting by the Finnish Police and the Ministry of Interior, there were 910 reported hate crime in 2018, a 22 % decline from the previous year. There was a spike in reported cases in 2015. It is unknown how many of these reported hate crimes would be classifiable as hate speech.[527]

forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.'

525 Päivi Korpisaari, 'Sananvapaus verkossa - yksilöön kohdistuva vihapuhe ja verkkoalustan ylläpitäjän vastuu' (2019) 117 Lakimies 928, 929-931.

526 Riku Neuvonen, Vihapuhe Suomessa (Edita Publishing Oy 2015) 28-29.

527 Jenita Rauta, Poliisin tietoon tullut viharikollisuus Suomessa 2018, <http://urn.fi/URN:NBN:fi-fe2019102935508> (Poliisiammattikorkeakoulun raportteja, Poliisiammattikorkeakoulu 2019) accessed 10 June 2020.

Generally, the term hate speech corresponds to the following criminal offenses in the Finnish criminal justice system: ethnic agitation[528], aggravated ethnic agitation[529], breach of sanctity of religion[530], menace[531], defamation[532] and dissemination of information violating personal privacy.[533] The Criminal Code also contains a provision for increasing the punishment due to a racist motive.[534]

Most typically, hate speech on the online environment is categorised as ethnic agitation in Finland. According to the Chapter 11, Section 10 of the Criminal Code, ethnic agitation includes 1) making available to the public or 2) otherwise spreading to the public or 3) keeping available public information, an expression of opinion or other messages where a certain group is threatened, defamed or insulted on the basis of its race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or a comparable basis. The provision covers all types of writings, pictures, drawings, videos and speeches.[535]

The category of making available to the public was added to the provision in 2011. The aim of the amendment was to take account the development of online environment. Making available means writing to a forum on the Internet, but also linking materials that otherwise fulfils the characteristics of an ethnic agitation.[536] The administrator is only required to remove a punitive post if the offence is directed against a group of people i.e. the offence could be considered as ethnic agitation. The responsibility of the administrator is concretised in situations where the provision contains the 'keep available' offence, which is only found in the provision on ethnic agitation of the offences listed above.[537]

Ethnic agitation and aggravated ethnic agitation are under public prosecution, but other offences mentioned above are complainant offences. The prosecutor can prosecute on certain complainant offences if a very important public interest so requires. Furthermore, the limitation of prosecution varies significantly in separate offences.[538] A person who has become the victim of a hate speech offence has a high threshold for reporting a crime. Most of the time the

528 Criminal Code of Finland (39/1889), ch 11 s 10.
529 Criminal Code of Finland (39/1889), ch 11 s 10a.
530 Criminal Code of Finland (39/1889), ch 17 s 10.
531 Criminal Code of Finland (39/1889), ch 25 s 7.
532 Criminal Code of Finland (39/1889), ch 24 s 9.
533 Criminal Code of Finland (39/1889), ch 24 s 8.
534 Criminal Code of Finland (39/1889), ch 6 s 5(1).
535 Government Proposal HE 317/2010 vp, 40.
536 Marko Forss, 'Rangaistava vihapuhe Internetissä- Miten kansanryhmän suoja eroaa yksilön suojasta?' [2018] 23 Edilex-sarja 5-6 <https://www.edilex.fi/artikkelit/18864 > accessed 1 March 2020.
537 Marko Forss, 'Rangaistava vihapuhe Internetissä- Miten kansanryhmän suoja eroaa yksilön suojasta?' [2018] 23 Edilex-sarja 15 <https://www.edilex.fi/artikkelit/18864> accessed 1 March 2020.
538 Marko Forss, 'Rangaistava vihapuhe Internetissä- Miten kansanryhmän suoja eroaa yksilön suojasta?' [2018] 23 Edilex-sarja 17 <https://www.edilex.fi/artikkelit/18864> accessed 1 March 2020.

complainant fears that taking a legal action would result in more negative attention.[539] Therefore, a large amount of hate speech is not prosecuted and in practise the aforementioned differences lead to a situation where the groups and individuals are treated differently concerning punishable hate speech.[540]

8.3. Adequate balance

The European Court of Human Rights has emphasised that Freedom of Expression is a part of the foundations in a democratic society.[541] Although penal provisions on hate speech and other racial crimes may violate fundamental and human rights, legislation concerning it must be in balance with Freedom of Expression.[542] The ECHR and the case law of European Court of Human Rights functions as a significant basis when evaluation the restriction of Freedom of Expression.[543]

The Finnish legislation and various international treaties restrict the exercise of Freedom of Expression so that it does not violate other fundamental rights or human dignity. Unlike the European Convention on Human Rights, the Constitution of Finland does not list the grounds exhaustively for restricting freedom of expression. However, the Constitutional Law Committee has written a list of criteria that may be applied when considering the restriction on Freedom of Expression. The list can be found in the legislative materials of the Finnish Constitution.[544]

Hate speech is not automatically regarded as an exercise of Freedom of Expression. The Finnish legislation does not recognise any prohibition of abuse of rights which would, in principle, exclude certain types of statements from Freedom of Expression. However, under the ECHR system, it is possible to both restrict the Rights guaranteed by the Convention[545] and completely exclude certain types of acts that are incompatible with the fundamental values of the Convention under the scope of protection.[546]

In addition to the ECHR-system, other international treaties and instruments have been created to prevent hate speech. Especially the Council of Europe has a significant role in adopting instruments that fight against discrimination. Many

539 Kari Mäkinen, Sanat ovat tekoja : Vihapuheen ja nettikiusaamisen vastaisten toimien tehostaminen. (Sisäministeriön julkaisuja 2019:23) 65.
540 Marko Forss, 'Rangaistava vihapuhe Internetissä- Miten kansanryhmän suoja eroaa yksilön suojasta?' [2018] 23 Edilex-sarja 17 <https://www.edilex.fi/artikkelit/18864> accessed 1 March 2020.
541 Anne Weber, Manual on Hate Speech (Council of Europe Publishing 2009) 2.
542 Statement of the Legal Affairs Committee LaVM 39/2010 vp, 3.
543 Anne Weber, Manual on Hate Speech (Council of Europe Publishing 2009) 19.
544 Riku Neuvonen, Vihapuhe Suomessa (Edita Publishing Oy 2015) 26-27.
545 European Convention on Human Rights, art 10, para 2.
546 ibid. art 17.

of the protocols and recommendations of the Council of Europe list several hate speech activities that should be penalised in the Member States. These instruments include for example The Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems and Declaration of the Committee of Ministers on Freedom of Political Debate in the Media and General Policy Recommendations of The European Commission against Racism and Intolerance (ECRI). Other instruments that include measures that help to decimate discrimination from our societies are for example European Social Charter and the Framework Convention for the Protection of National Minorities.[547] In addition, the Committee of Ministers has presented in its Recommendation (97)20 on 'hate speech' that freedom of expression should be restricted as narrowly as possible and be subjected to judicial control. The Recommendation also instructs that authorities should take regulation on freedom of expression and the principle of proportionality carefully into account when imposing criminal sanctions on hate speech.[548]

Furthermore, the Charter of Fundamental Rights of the European Union recognises freedom of expression in Article 11 and the right to non-discrimination in Article 21. Fight against discrimination is one of the key points in the EU's policies and it is reflected in the Union's strategy in combating racism.[549] The European Commission has also published Commission Recommendation (EU 2018/334) on Measures to Effectively Tackle Illegal Content Online to prevent illegal content from spreading in online environment. In addition, the EU has created Code of conduct on countering illegal hate speech online to prevent and protect against online hate speech. IT companies such as Facebook, Microsoft, Twitter, and YouTube have signed and agreed for instance to have rules and community standards that prohibit hate speech and put in place systems and teams to review content that is reported.[550]

Overall, the general guidelines in Europe deem that the Right to Freedom of Expression should be restricted in order to protect against hate speech as long as the restriction fulfils the requirements set out in the ECHR. Particularly the

547 Anne Weber, Manual on Hate Speech (Council of Europe Publishing 2009) 7-10, 12.

548 Recommendation No. R (97) 20 Of the Committee Of Ministers To Member States On 'Hate Speech', Principle 5 (adopted by the Committee of Ministers on 30 October 1997, at the 607th meeting of the Minister's Deputies) <https://rm.coe.int/1680505d5b> accessed 24 January 2020.

549 Anne Weber, Manual on Hate Speech (Council of Europe Publishing 2009) 15.

550 European Commission, The EU Code of conduct on countering illegal hate speechonline <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 18 March 2020.

rights and reputation of others are respected and violations against them are seen inadmissible.

8.4. Fight against hate speech in Finland

The Finnish authorities have taken many steps to combat hate speech. For example, the Ministry of the Interior, the Ministry of Justice and the Ministry of Education and Culture launched a project in 2018 with the task of drafting proposals for more efficient measures against hate speech and harassment. At the end of the project, the working group presented 13 different recommendations for the fight against hate speech.[551] The recommendations that this working group suggested have already been activated since several measures against hate crime and hate speech have been outlined in Prime Minister Sanna Marin's Government Programme, such as drafting of an action plan against racism and discrimination.[552] At the moment, the Ministry of Justice is launching a new project called Facts Against Hate. The project focuses on four targets for development: hate crime reporting, local cooperation practices, hate crime monitoring and transnational and EU-level cooperation.[553]

Most of the hate speech is concentrated in online platforms and the Finnish legislation has not kept up with the evolution of online hate speech. Therefore, legislators should consider making Commission Recommendation (EU 2018/334) on Measures to Effectively Tackle Illegal Content Online more binding to online service providers. Overall transparency and moderation should be improved in these platforms. The expert working group suggested that online platforms could be obliged to remove clearly penalised online content and to provide a reasoned reply to the notifier within a reasonable time. Furthermore, it should also be assessed whether the terms of use of the online platforms should prohibit the spreading of illegal and punitive hate speech in the service and should the online platforms monitor the use of anonymous accounts.[554]

Many issues need more attention in the Finnish Criminal Code concerning hate crimes. However, one of the key differences between Finland and several other EU countries is that the Finnish legislation does not separately criminalise

551 Kari Mäkinen, Sanat ovat tekoja : Vihapuheen ja nettikiusaamisen vastaisten toimien tehostaminen. (Sisäministeriön julkaisuja 2019:23) Description Sheet.

552 The Finnish Government, Programme of Prime Minister Sanna Marin's Government 10 December 2019. Inclusive and competent Finland – a socially, economically and ecologically sustainable society (Valtioneuvoston julkaisuja 2019:31).

553 Ministry of Justice, Facts Against Hate, <https://oikeusministerio.fi/hanke?tunnus=OM043:00/2019> accessed 13 February 2020.

554 Kari Mäkinen, Sanat ovat tekoja : Vihapuheen ja nettikiusaamisen vastaisten toimien tehostaminen. (Sisäministeriön julkaisuja 2019:23) 67.

denying genocide.[555] The European Court of has several occasions expressed that historical negationism especially concerning the holocaust is against the fundamental values of the European Convention of Human Rights.[556] In the absence of separate criminalisation on denying genocide, the position of the legislature is unclear. It is also important to note that the view of European Court of Human Rights cannot have a wide-ranging impact on the application of domestic law.[557] As the provision on ethnic agitation has been written in general form, it is difficult to say with certainty whether it would be applicable. For this reason, a specific criminal provision on denying genocide should be added to the legislation. This action would present a dedication to the fundamental values of Europe.

Due to its revision in 2011, the provision on ethnic agitation takes offences in online environment more account. It is obvious that one provision cannot measure up to all the manifestations of online hate speech. A large amount of hate speech that is concentrated on individuals are not prosecuted since they do not fall under the application of ethnic agitation. This is a large gap in the legislation since the rights of the individuals are of equal value to the rights of groups. Furthermore, as mentioned above, there is also a need for evaluating if hate crimes should be transferred under public prosecution to ensure that appropriate prosecution and sanctions are taken against those that are responsible for these acts.

Concentrating more on the victims of hate speech entails the European point of view. Therefore, raising awareness of legal remedies available in cases of hate crime and increasing information on appropriate prosecution and sanction measures to those responsible for these acts could help to combat hate speech. Increasing legislative action is not necessarily the most effective option, as Freedom of Expression must be strongly considered when addressing hate speech. Thus, a better solution could be found in increasing information, research projects and education on hate speech and the limits of freedom of expression. ECRI recommended in a Report on Finland (CRI(2019)38) published on 10 September 2019 that the Finnish authorities should create an inter-institutional working group to develop a comprehensive strategy for tackling hate speech and make efforts to condemn hate speech in public discourse.

---

555 Kimmo Nuotio, Vihapuheen rikosoikeudellinen sääntely in book Riku Neuvonen (ed.), Vihapuhe Suomessa (Edita Publishing oy 2015) 160.

556 Anne Weber, Manual on Hate Speech (Council of Europe Publishing 2009) 24.

557 Kimmo Nuotio, Vihapuheen rikosoikeudellinen sääntely in book Riku Neuvonen (ed.), Vihapuhe Suomessa (Edita Publishing oy 2015) 160.

Reaching balance between allowing Freedom of Expression and protecting against hate speech is more complicated than one could think. States have the responsibility to honour equality and respect all of its members which includes people who might have racist opinions. Legislative measures to combat hate speech could also be seen as a danger for governments to abuse their powers to screen out expressions that are against their policies. Preserving the victims' rights to human dignity is seen as a core value in our society.

Overall, the key point of view in Finland is that Freedom of Expression should be restricted as narrowly as possible and be subjected to the judicial control of the authorities and courts. Therefore, the Finnish courts play a significant role when defining the balance between Freedom of Expression and hate speech. The Finnish Supreme Court has ruled that imposing a penalty for ethnic agitation, attention must be paid to the quality and nature of the expressions used. Thus, an act that involves incitement to direct violence or an expression that comes across as threat-like could be considered more reprehensible.[558] This is in line with the case law of ECtHR. As mentioned above the Finnish legislation does not recognise the prohibition of abuse of rights. Hence, hate speech has not been seen as a fundamental abuse of Freedom Expression in the Finnish legal practise. However, Finnish courts have recently begun to take a more permissive approach to the grounds for restricting Freedom of Expression and take to account the case law of ECtHR in their judgments.[559]

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

Fundamental (constitutional) rights and human rights can sometimes be in conflict with each other. Their correct application therefore requires a careful balancing act and the weighing in of the different interests in question. This is also the case for the Right to the Freedom of Expression, which might collide with, for instance, the Right to Dignity. As discussed under question 8, there are limitations to Freedom of Expression when it comes to hate speech: not all kinds of expression enjoy equal legal protection.

558 Supreme Court of Finland, KKO 2012:58, 8 June 2012.

559 For example, KKO 2012:58 (judgment of the Supreme Court); Kouvolan HO, 12.12.2011, 1146 (judgement of the Court of Appeal in Kouvola).

9.1. Right to privacy

The Right to the respect for private and family life is protected under both Article 8 of the ECHR and the Section 10 of the Finnish Constitution. Everyone's private life, honour and the sanctity of the home are protected, as are the secrecy of correspondence, telephony, and other confidential communications. Communications protected by the constitution include emails, text messages and other digital forms of communication. In 2018, an amendment was made to the Finnish law, enabling limitations to the secrecy of communications if they are necessary for the investigation of a threat to national security.

Disturbance of the sanctity of communications (as a form of sanctity of the home) is criminalised in the Criminal Code chapter 24 Section 1a. The criminalised activity is described as repeatedly calling or sending messages in a manner that is conducive to disturbing the recipient. This is a fairly recent addition from 2009 and extends the sanctity of the home to also include digital platforms to a certain extent. It can be considered a restriction on free expression (as for example chat messages are a form of expression) but it is a welcome addition as prior to its enactment, the criminal statute did not have a provision criminalising such activity.

Honour (or reputation) is protected by laws prohibiting dissemination of information violating personal privacy (Criminal Statute Section 8) and defamation (Criminal Statute Section 9).

The important distinction between the two is that the first is specifically dissemination that has to violate personal privacy, not the information itself. That is to say that the information itself need not be in violation of the target's honour or privacy. The rationale is that for example disseminating correct information about someone, such as someone's criminal record, can be criminal even though the information itself is public and correct, if it is done with malicious intent and the subject has suffered harm due to the dissemination of said information.

Defamation, on the other hand, consists of either false information, false insinuation or some other type of disparagement.

9.2. Defamation in online spaces

There are no separate provisions for online speech as freedom of expression is medium neutral. The dissemination section has been applied to, for example, a

shopkeeper uploading a photo and a video of a minor committing theft to the store's Facebook page.[560]

As lay people now have the means to broadcast defamatory messages and images without editorial oversight on social media and online in general, it is likely that defamation and dissemination of information violating personal privacy cases become more numerous between individuals. For example, doxxing could be considered a dissemination crime (see question 7 for discussion on related legislative efforts). In the past these crimes mainly occurred in commercially published materials, as shown by Finland having several judgements from the ECtHR concerning sanctions posed on members of the press under these criminal statutes.

Anonymity provided by online platforms further exacerbates the problem of online violations of privacy or honour, as the real-life culprit can be impossible to track down. Another aspect is online vigilantism; the Finnish police has warned against sharing tips or information on social media purported to relate to a crime as such activity lends itself quite easily to violations of privacy.[561] Two recent Supreme court cases have dealt with balancing the Right to Privacy with Right to Free Speech. In 2018, the Court condemned the publication of the photo of a convicted paedophile in a Facebook group as 'morally dubious' and had crossed the line of what is socially acceptable. However, the information had been previously available and it could be considered to be of public interest so it was covered as free speech, regardless of what effect the dissemination had on the subject.[562] In 2019 discussions relating to someone 'harbouring paedophiles' on an online forum were ordered to be removed.[563] In both cases, the Court has had to consider when defamatory speech becomes intolerable in regards to the subject's Right to Privacy. The cases are complementary to each other rather than a change in precedent. They go to show that protection for even morally scrupulous speech be waived only when it crosses a very strict threshold.

9.3. Freedom of religion

Freedom of Religion and Conscience is guaranteed by Article 9 of ECtHR and Section 11 of the Constitution of Finland. The Freedom of Expression and

560 Iltalehti: Kauppias latasi videon alaikäisestä 'juoksujuoman hakijasta' kauppansa Facebook-sivuille – tuomio tuli, kauppias joutuu maksamaan teinipojalle 1500 euron korvaukset <https://www.iltalehti.fi/kotimaa/a/20180719220108398 3> accessed 10 June 2020.

561 Poliisi: Mieti, mitä julkaiset sosiaalisessa mediassa – älä syyllisty rikokseen! <https://www.poliisi.fi/sisa-suomi/tiedotteet/1/0/mieti_mita_julkaiset_sosiaalisessa_mediassa_-_ala_syyllisty_rikokseen_88098> accessed 10 June 2020.

562 Korkein oikeus 2018:51 päätöslauselma.

563 Korkein oikeus 2019:81.

criticism of religion or of religious figures has been duly discussed in question 8 regarding hate speech.

Of note is that in addition to agitation crimes, breach of the sanctity of religion is also criminalised under Chapter 17 of the Criminal Code, titled 'Offences against public order'. Section 10 of the Chapter reads (in part) that it is illegal to publicly blaspheme against God or, for the purpose of offending, publicly defame or desecrate what is otherwise held to be sacred by a church or religious community. Therefore, blasphemy is still technically a criminal offense, a rather antiquated limitation to the freedom of expression.

9.4. Discussion

The Freedom of Expression enjoys a high level of protection in Finland, particularly when it comes to matters of public opinion and journalistic freedom. Restrictions to speech are considered fairly narrowly (see 9.2 discussion of precedent). Online spaces have allowed more people to easily disseminate information given rise to potential defamation and related crimes. The discussion seems to be around how to 'sanitise the Internet' which is hard to do on a national level. Finland still holds on to a strict application of limits to free speech, even when the speech is deemed socially unacceptable.

A recent development is the National Prosecuting Authority seeking permission from the Parliament to raise charges against a member of parliament regarding his comments made in session, something that has never been done before given the high level of protection members of parliament enjoy in regard to their speech.

10. How do you rank the access to freedom of expression online in your country?

Access to Freedom of Expression online can be thought to consist of two factors: the Right to Internet Access, and the Right to express and access views and opinions (while on the Internet). In my opinion, Finland should be ranked among the very top when it comes to the freedom of expression online. reasons for this are given below.

The general situation with Freedom of Expression has been comprehensively discussed in the previous chapters. Among other things, Finland has consistently ranked among the top in the Reporters Without Borders Press Freedom Index which that evaluates the independence and pluralism of media, the free flow of information, legality, security, and freedom of authors. The general picture is

that anyone can express themselves in social media and get the information freely online in Finland.

The Right to Internet access, also known as 'the Right to broadband' or 'the freedom to connect', is the view that all people must be able to access the Internet in order to exercise and enjoy their rights to freedom of expression and opinion and other fundamental human rights. According to this view, states have a responsibility to ensure the broad availability of access to Internet, and that this access may not be unreasonably restricted.

While some countries and international organisations, such as the United Nations, generally recognise Internet access as important tool for the Freedom of Expression, others have chosen the path of content and access blocking measures. Among the former group, a handful of countries stand out in particular for having ruled that access to the Internet is not only a practical tool to fulfil other rights, but a fundamental citizen's right in its own right.

Since 2010, Finland has considered Internet access a legal right, not a privilege. The government's reasoning was that the Internet has become an essential part of modern society, just as much as water or electricity. This Right entails the concrete Right to a specific connection speed. While Finns still have to pay for the broadband companies to access the Internet in their homes, basic social assistance is available to individuals and families whose income and assets do not cover their essential daily expenses – such as the Internet. Government and community projects are bringing high-speed fibre optic broadband to remote areas. Furthermore, the Finns can freely access the Internet at various public schools, universities, and libraries.

Finland has specific legal provisions guaranteeing or regulating 'net neutrality' in its jurisdiction. In Finland, since July 2010, subject to section 60(3) of the Communications Market Act, all Finnish citizens have a legal Right to access a one megabit per second broadband connection, reportedly making Finland the first country to accord such a Right.[564] Network neutrality is an important prerequisite for the Internet to be equally accessible and affordable to all. Most of the EU states do not have legal provisions in place to guarantee net neutrality. Finland stands out as the best practice example, because Finland has anchored network neutrality in its corpus of laws.

---

564 Finnish Ministry of Transport and Communications Press Release, 1 Mbit Internet access a universal service in Finland from the beginning of July, 29.06.2010, at : 'The Ministry of Transport and Communications has defined the minimum rate of downstream traffic of a functional Internet access to be 1 Mbit/s, and the Finnish Communications Regulatory Authority, FICORA, has defined 26 telecom operators across Finland as universal service operators.'

In Finland, for the purpose of prohibiting Internet piracy, the author or his representative has the right to take legal action against the person who makes the allegedly copyright-infringing material available to the public. In allowing such action, the Court of Justice, at the same time may order that the making available of the material to the public must cease. The Court of Justice may impose a conditional fine to reinforce the order. The Court of Justice may, upon the request of the author or his representative, order the maintainer of the transmitter, server or other device or any other service provider acting as an intermediary to discontinue, on paying a fine, the making of the allegedly copyright-infringing material available to the public (injunction to discontinue), unless this can be regarded as unreasonable in view of the rights of the person making the material available to the public, the intermediary, and the author. Criminal liability for infringement of copyright also exists in Finland.

In Finland, defamation is criminalised in the Criminal Code, and a person who spreads false information or a false insinuation of another person so that the act is conducive to causing damage or suffering to that person, or subjecting that person to contempt, or disparages another in a manner other than referred above shall be sentenced for defamation to a fine or to imprisonment of up to six months. Criticism that is directed at a person's activities in politics, business, public office, public position, science, art or in comparable public activity and that does not obviously overstep the limits of propriety does not constitute defamation.

In Finland, ISP liability provisions exist. These are in line with the EU e-Commerce Directive requirements. The Directive was transposed into national law with the Act on Provision of Information Society Services (458/2002). Chapter 4 of the Act exempts service providers, acting as intermediaries, from liability. The service provider's exemption from liability shall have no effect on its obligation, under any other law, to take necessary action to implement an order or a decision by a court or by any other competent authority. The Act also contains provisions on notice and take-down. However, the notice and take-down provisions are applicable only to the hosting of services.

Finland also has some of the lowest rates of Internet censorship and regulation, with only illegal or dangerous websites being banned. For instance, some Finnish Internet Service Providers automatically block access to pirating websites. Legal provisions for blocking access to known child pornography websites exist in Finland. At EU level, 'mandatory blocking' of websites containing child pornography was not recommended but the member states 'may take the necessary measures in accordance with national legislation to prevent access to

such content in their territory'. There have been a few issues with this. Hotlines to which allegedly illegal Internet content can be reported, have been developed in Finland. According to a EuroBarometer Survey of 2008, reporting to the hotlines seems to be low and users seem to prefer to report illegal content they come across to the police rather than to hotlines. Liability provisions for service providers are not always clear and complex notice and take-down provisions exist for content removal from the Internet within Finland. Regarding the formation of public or private hotlines, it should be noted that although hotlines could potentially play an important role in relation to illegal Internet content, there remain significant questions about their operation. Private hotlines are often criticised as there remain serious concerns regarding the 'policing' role they might play. The lack of transparency regarding the work of hotlines often attracts accusations of censorship, and Finland is no exception.[565] Wikileaks have confirmed that most of the hotlines block access to adult pornographic content and even political content. In the absence of openness and transparency of the work of hotlines and by creating secrecy surrounding the blocking criteria and keeping the list of blocked websites confidential, concerns will continue to exist. The hotlines can only refute such criticism if they are established within a regulatory framework that is compatible with the requirements of the European Convention on Human Rights and other internationally applicable standards, including OSCE commitments.

Despite the fact and accusation from Wikileaks, Finland has been successful in establishing access to the Internet. In Finland the Internet is free and available to everyone, anyone can express themselves effectively online and get any information from the Internet. There is right against harassment, defamation and fake news. Hence Finland deserves the highest grade.

11. How do you overall assess the legal situation in your country regarding Internet censorship?

The International Human Rights Treaties binding to Finland and the Finnish Constitution Section 12 on Freedom of Expression provide frame for Internet content restrictions. In Finland, ex ante restrictions of Freedom of Expression are prohibited. The Finnish Criminal Code sets limitations to Freedom of Expression, for example defamation and Freedom of Expression, in order to

[565] Wikileaks, '797 domains on Finnish Internet censorship list, including censorship critic, 2008,' 5 January, 2009 <https://www.wikileaks.com/wiki/797_domains_on_Finnish_Internet_censorship_list%2C> accessed 10 June 2020.

secure peace. However, hate crime and hate speech lack clear definition in Finnish legislation. Many projects have been initiated to fight hate speech. In addition, the Government Programme outlines several measures against hate crime and hate speech, such as drafting of an action plan against racism and discrimination. Criminalisation of targeting in one form or another is expected in near future as well. Finland has positioned itself as an advocate for digital privacy rights though this might not translate into further national legislation.

Virtual private networks are not prohibited by law in Finland. Illegal content is provided in several legislations (see question 2 for details). Generally, censorship should always be based on a court order. However, special legislation provides powers for Finnish authorities to block foreign websites containing child abuse material. No specific jurisdiction on public content on social media is provided in Finland. The Information Society Code of Finland does define information services liable for public consent. Self-regulation of company websites depends highly on company values and whether or not a national self-regulating committee has been established for each of specific private sector. The Council for Mass Media has issued Guidelines for Journalists and the Council of Ethics in Advertising for marketing and commercial companies. These guidelines apply also when publishing on Internet platforms. Freedom of Expression may be affected by use of different models when publishing online discussions on private sector forums and websites since those practices are purely based on information service's own rules. The Right to Anonymous Expression is protected by the exercise of Freedom of Expression in the mass media in Finland[566]. Quick, easy publication in the Internet and anonymity have resulted in an increase of hate messages and made it more difficult to identify and hold accountable those sending messages.[567]

Finland is an EU Member State. Thus, EU law takes primacy over national law. Even though the GDPR is supplemented with national legislation, there is no special legislation for the right to be forgotten. The Data Protection Ombudsman takes into account national law, CJEU case law, ECtHR case law and WP29 guidelines in particular when making a judgement. In most of the cases three legal questions arise based on principles provided by the WP29 guidelines. Firstly, does the data subject play a role in public life and is the data subject a public figure? Secondly, is the information of the data subject currently irrelevant, inaccurate, incomplete or outdated for the purpose of the processing of personal data? And thirdly, should the order be given by the DPO to correct

566 Sananvapauslaki 13.6.2003/460, Chapter 4, Section 16.

567 Päivi, Korpisaari. Sananvapaus verkossa -yksilöön kohdistuva vihapuhe ja vekkoalustan ylläpitäjän vastuu. Lakimies 7-8/2009. 933.

(i.e. delete) the information? The DPO does not assess whether exercising Freedom of Expression has led to overstatement or even criminal offence since that is ultimately a matter for the court.[568]

The Finnish legislation provides a strong protection to the freedom of expression. Reporters without borders call Finland the 'land of the free press'. Finland has also been continuously ranked as one of the best countries in the World Press Freedom Index. However, the ECtHR has provided judgements on 20 freedom of expression violations between 2002 and 2019.[569] In most of the cases the plaintiffs are well-known journalists in some of the central publication houses in Finland. Complaints indicate a disagreement between the State of Finland and the well-established media on scope of freedom of expression. In many cases violations arise from cases where media has published unfavourable information of a public person, for example five cases concerned a prior National Conciliator.[570] In these cases, the Court held that the public interest prevails the right to privacy of ordinary citizens. Therefore, providing heavy criminal sanctions to journalists or media houses would not be proportionate in relation to the acceptable aims for restricting freedom of expression.

A significant turning point was marked by the ECtHR judgement on 14 January 2014 in the cases *Ruusunen v. Finland and Ojala* and *Etukeno Oy v. Finland*.[571] The national Supreme Court judgment provided extensive reasoning of the role of the Prime Minister in society and how it affects their right to privacy in relation to the freedom of expression.[572] Reasoning also included highly detailed arguments on grounds of criminal sanctions in addition to relevant ECtHR

---

568 Docket no 1379/533/2018, 27.9.2018; Docket no 3668/533/2017, 12.7.2018; Docket no 1374/533/2015, 3.12.2015.

569 *Nikula v. Finland* App no 31611/96 (ECtHR, 21.6.2002), *Selistö v. Finland* App no 56767/00 (ECtHR, 16.2.2005), *Karhuvaara and Iltalehti v. Finland* App no 53678/00 (ECHR, 16.2.2005), *Goussev and Marek v. Finland* App no 35083/97 (ECHR, 17.4.2006), *Soini and Others v. Finland* App no 36404/97 (ECHR, 17.4.2006), *Juppala v. Finland* App no 18620/03 (ECHR, 2.3.2009), *Eerikäinen and Others v. Finland* App no 3514/02 (ECHR, 13.3.2009), *Flinkkilä v. Finland* App no 25576/04 (ECHR, 6.7.2010), *Jokitaipale and Others v. Finland* App no 3349/05 (ECHR, 6.7.2010), *Iltalehti and Karhuvaara v. Finland* App no 6372/06 (ECHR, 6.7.2010), *Soila v. Finland* App no 25711/04 (ECHR, 6.7.2010), *Tuomela and Others v. Finland* App no 25711/04 (ECHR, 6.7.2010), *Niskasaari and Others v. Finland* App no 37520/07 (ECHR, 6.10.2010), *Maripori v. Finland* App no 37751/07 (ECHR, 6.10.2010), *Saaristo and Others v. Finland* App no 184/06 (ECHR, 12.1.2011), *Reinboth and Others v. Finland* App no 30865/08 (ECHR, 25.4.2011), *Lahtonen v. Finland* App no 29576/09 (ECtHR, 17.4.2012), *Ristamäki and Korvola v. Finland* App no 66456/09 (ECHR, 29.1.2014), *Niskasaari and Otavamedia Oy v. Finland* App no 32297/10 (ECHR, 25.6.2015) *M.P. v. Finland* App no 36487/12 (ECHR, 15.3.2017).

570 Flinkkilä v. Finland App no 25576/04 (ECtHR, 6.7.2010), Jokitaipale and Others v. Finland App no 3349/05 (ECtHR, 6.7.2010), Iltalehti and Karhuvaara v. Finland App no 6372/06 (ECtHR, 6.7.2010), Soila v. Finland App no 25711/04 (ECtHR, 6.7.2010), Tuomela and Others v. Finland App no 25711/04 (ECtHR, 6.7.2010).

571 Ruusunen v. Finland App no 73579/10 (ECtHR, 14.1.2014) and Ojala and Etukeno Oy v. Finland App no 68839/10 (ECtHR, 14.1.2014).

572 KKO:2010:39.

judgements in its ruling. The ECtHR made a distinction between monetary sanctions and other forms of criminal sanctions since monetary sanction does not provide a criminal record. This argumentation has later resulted in non-violation judgements by the ECtHR.[573] When considering the consequences of this approach, it should be noted that Finland is a trust society. This means that the penal policy has a clear social orientation that reflect the values of Nordic welfare state and fight against marginalisation and inequality, in addition to crime. Tolerant policies promote trust and legitimacy making it possible to maintain alternatives to imprisonment, such as monetary sanctions. This Nordic leniency is strongly influenced by experts, sensible media and demographic homogeneity.[574] In Finland, punishment, not excluding monetary sanction, reflects disapproval and is assumed to influence the values, morals and actions of individuals.[575]

[573] Salumäki v. Finland App no 23605/09 (ECtHR, 29.4.2014), Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland App no 931/13 (ECtHR, 21.7.2015), Pentikäinen v. Finland App no 11882/10 (ECtHR, 20.10.2015).

[574] Nuotio, Kimmo. Reason for Maintaining the Diversity. – L´Harmonisation des sanctions pénales en Europe. Delmas-Marty, M (edit.). Société de Legislation Compare. Paris. 2003. Vol.6. 465.

[575] Lappi-Seppälä, Tapio. Penal Policy in Scandinavia. – Crime and Justice. A Review of Research. 2007. Vol. 36. No 1. The University of Chicago Press Journals. Chicago. 232.

Table of legislation

Provision in Finnish	**Corresponding translation in English**
Rikoslaki (39/1889), Luku 25, 7 § Laiton uhkaus Joka nostaa aseen toista vastaan tai muulla tavoin uhkaa toista rikoksella sellaisissa olosuhteissa, että uhatulla on perusteltu syy omasta tai toisen puolesta pelätä henkilökohtaisen turvallisuuden tai omaisuuden olevan vakavassa vaarassa, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa rangaistusta, laittomasta uhkauksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi	The Criminal Code of Finland (39/1889), Chapter 25 Section 7 Menace A person who raises a weapon at another or otherwise threatens another with an offence under such circumstances that the person so threatened has justified reason to believe that his or her personal safety or property or that of someone else is in serious danger shall, unless a more severe penalty has been provided elsewhere in law for the act, be sentenced for menace to a fine or to imprisonment for at most two years.
Rikoslaki (39/1889), Luku 24, 9 § Kunnianloukkaus Joka 1) esittää toisesta valheellisen tiedon tai vihjauksen siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, taikka 2) muuten kuin 1 kohdassa tarkoitetulla tavalla halventaa toista, on tuomittava kunnianloukkauksesta sakkoon. Kunnianloukkauksesta tuomitaan myös se, joka esittää kuolleesta henkilöstä valheellisen tiedon tai vihjauksen siten, että teko on omiaan aiheuttamaan kärsimystä ihmiselle, jolle vainaja oli erityisen läheinen. Edellä 1 momentin 2 kohdassa tarkoitettuna kunnianloukkauksena ei pidetä arvostelua, joka kohdistuu toisen menettelyyn politiikassa, elinkeinoelämässä, julkisessa virassa tai tehtävässä, tieteessä, taiteessa taikka näihin rinnastettavassa julkisessa toiminnassa ja joka ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä. Kunnianloukkauksena ei myöskään pidetä yleiseltä kannalta merkittävän asian käsittelemiseksi esitettyä ilmaisua, jos sen esittäminen, huomioon ottaen sen sisältö, toisten oikeudet ja muut olosuhteet, ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä.	The Criminal Code of Finland (39/1889), Chapter 24 Section 9 Defamation (879/2013) (1) A person who (1) spreads false information or a false insinuation of another person so that the act is conducive to causing damage or suffering to that person, or subjecting that person to contempt, or (2) disparages another in a manner other than referred to in paragraph (1) shall be sentenced for defamation to a fine. (2) Also a person who spreads false information or a false insinuation about a deceased person, so that the act is conducive to causing suffering to a person to whom the deceased was particularly close, shall be sentenced for defamation. (3) Criticism that is directed at a person's activities in politics, business, public office, public position, science, art or in comparable public activity and that does not obviously exceed the limits of propriety does not constitute defamation referred to in subsection 1(2). (4) Presentation of an expression in the consideration of a matter of general importance shall also not be considered defamation if its presentation, taking into. consideration its contents, the rights of others and the other circumstances, does not clearly exceed what can be deemed acceptable.

Rikoslaki (39/1889), Luku 11, 10 § Kiihottaminen kansanryhmää vastaan Joka asettaa yleisön saataville tai muutoin yleisön keskuuteen levittää tai pitää yleisön saatavilla tiedon, mielipiteen tai muun viestin, jossa uhataan, panetellaan tai solvataan jotakin ryhmää rodun, ihonvärin, syntyperän, kansallisen tai etnisen alkuperän, uskonnon tai vakaumuksen, seksuaalisen suuntautumisen tai vammaisuuden perusteella taikka niihin rinnastettavalla muulla perusteella, on tuomittava kiihottamisesta kansanryhmää vastaan sakkoon tai vankeuteen enintään kahdeksi vuodeksi.	The Criminal Code of Finland (39/1889), Chapter 11 Section 10 Ethnic Agitation A person who makes available to the public or otherwise spreads among the public or keeps available for the public information, an expression of opinion or another message where a certain group is threatened, defamed or insulted on the basis of its race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or a comparable basis, shall be sentenced for ethnic agitation to a fine or to imprisonment for at most two years.
Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lisäpöytäkirjan, joka koskee tietojärjestelmien välityksellä tehtyjen luonteeltaan rasististen ja muukalaisvihamielisten tekojen kriminalisointia, hyväksymisestä ja laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain ja tietoyhteiskunnan palvelujen tarjoamisesta annetun lain 15 §:n muuttamisesta (HE 317/2010)	Government Proposal to Parliament for Approval of the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems and for an Act on the Assertation of Provisions Included in the Legislation in question and for Amending the Criminal Code and Section 15 of the Act on Provision of Information Society Services (HE 317/2010)
Tietosuojalaki (1050/2018) § 27 Henkilötietojen käsittely journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten. Sananvapauden ja tiedonvälityksen vapauden turvaamiseksi henkilötietojen käsittelyyn ainoastaan journalistisia tarkoituksia varten tai akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten ei sovelleta tietosuoja-asetuksen 5 artiklan 1 kohdan c–e alakohtaa, 6 ja 7 artiklaa, 9 ja 10 artiklaa, 11 artiklan 2 kohtaa, 12–22 artiklaa, 30 artiklaa, 34 artiklan 1–3 kohtaa, 35 ja 36 artiklaa, 56 artiklaa, 58 artiklan 2 kohdan f alakohtaa, 60–63 artiklaa ja 65–67 artiklaa.Tietosuoja-asetuksen 27 artiklaa ei sovelleta sellaiseen henkilötietojen käsittelyyn, joka liittyy sananvapauden käyttämisestä joukkoviestinnässä annetussa laissa (460/2003) säädettyyn toimintaan. Tietosuoja-asetuksen 44–50 artiklaa ei sovelleta, jos soveltaminen loukkaisi oikeutta sananvapauteen tai tiedonvälityksen	Data Protection Act (1050/2018) Section 27 Processing of personal data for the purposes of journalistic, academic, artistic or written expression. In order to ensure freedom of expression and information, Articles 5 (1) (c) to (e), 6 and 7, 9 and 10, 11 (2), –Article 22, Article 30, Article 34 (1) to (3), Articles 35 and 36, Article 56, Article 58 (2) (f), Articles 60 to 63 and Articles 65 to 67. Article 27 of the Data Protection Regulation shall not apply to the processing of personal data, relating to the activities provided for in the Act on the Exercise of Freedom of Expression in the Mass Media (460/2003). Articles 44 to 50 of the Data Protection Regulation shall not apply if the application would infringe the right to freedom of expression or information. paragraphs 2 and 2, Articles 24 to 26, 31, 39 and 40, 42, 57 and 58, 64 and 70 only where applicable.

vapauteen.Sananvapauden ja tiedonvälityksen vapauden turvaamiseksi henkilötietojen käsittelyyn ainoastaan journalistisia tarkoituksia varten tai akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten sovelletaan tietosuoja-asetuksen 5 artiklan 1 kohdan a ja b alakohtaa ja 2 kohtaa, 24–26 artiklaa, 31 artiklaa, 39 ja 40 artiklaa, 42 artiklaa, 57 ja 58 artiklaa, 64 artiklaa ja 70 artiklaa ainoastaan soveltuvin osin.	
Tietoyhteiskuntakaari (917/2014), Luku 22, 183 §	Information Society Code (917/2014), Chapter 22, section 183 Exemption from liability when caching the information When an information society service consists of the transfer in a communications network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, if the service provider: 1) does not modify the information; 2) complies with the conditions on access to the information; 3) complies with rules regarding the updating of the information, specified in a manner widely recognised and used in the industry; 4) does not interfere with the lawful use of technology, widely recognised and used in the industry, to obtain data on the use of the information; and 5) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact: a) that the information at the initial source of the transmission has been removed from the network; b) access to it has been disabled; or c) a court or an administrative authority has ordered such removal or disablement.
Tietoyhteiskuntakaari (917/2014), Luku 22, 184 § Vastuuvapaus tietojen tallennuspalveluissa Kun tietoyhteiskunnan palvelu käsittää palvelun vastaanottajan (sisällön tuottaja) toimittamien tietojen tallentamisen tämän	Information Society Code (917/2014), Chapter 22, section 184 Exemption from liability in hosting services When an information society service consists of the storage of information provided by a recipient (content provider) of

pyynnöstä, palvelun tarjoaja ei ole vastuussa tallennettujen tietojen sisällöstä tai välittämisestä, jos hän toimii viipymättä tallentamansa tiedon saannin estämiseksi saatuaan: 1) tietoonsa sitä koskevan tuomioistuimen määräyksen taikka, jos kysymyksessä on tekijänoikeuden tai lähioikeuden loukkaaminen, saatuaan 191 §:ssä tarkoitetun ilmoituksen; 2) muuten tosiasiallisesti tietoonsa, että tallennettu tieto on ilmeisesti rikoslain 11 luvun 10 tai 10 a §:n taikka 17 luvun 18 tai 18 a §:n vastainen. Mitä 1 momentissa säädetään, ei sovelleta, jos sisällön tuottaja toimii palvelun tarjoajan johdon tai valvonnan alaisena.	the service upon his request, the service provider is not liable for the content of the information stored or transmitted at the request of a recipient of the service if it acts expeditiously to disable access to the information stored upon: 1) obtaining knowledge of a court order concerning it or if it concerns violation of copyright or neighbouring right upon obtaining the notification referred to in section 191; 2) otherwise obtaining actual knowledge of the fact that the stored information is clearly contrary to section 10 or 10(a) of Chapter 11 or section 18 or 18(a) of Chapter 17 of the Criminal Code. The provisions in subsection 1 shall not apply if the content provider is acting under the authority or the control of the service provider.
Tietoyhteiskuntakaari (917/2014), Luku 22, 185 § Tiedon saannin estoa koskeva määräys Käräjäoikeus voi syyttäjän tai tutkinnanjohtajan hakemuksesta taikka sen hakemuksesta, jonka oikeutta asia koskee, määrätä 184 §:ssä tarkoitetun tietoyhteiskunnan palvelun tarjoajan sakon uhalla estämään tallentamansa tiedon saannin, jos tieto on ilmeisesti sellainen, että sen sisällön pitäminen yleisön saatavilla tai sen välittäminen on säädetty rangaistavaksi tai korvausvastuun perusteeksi. Hakemus on käsiteltävä kiireellisesti. Hakemusta ei voida hyväksyä varaamatta palvelun tarjoajalle ja sisällön tuottajalle tilaisuutta tulla kuulluksi, paitsi jos kuulemista ei voida toimittaa niin nopeasti kuin asian kiireellisyys välttämättä vaatii. Käräjäoikeuden määräys on annettava tiedoksi myös sisällön tuottajalle. Jos sisällöntuottaja on tuntematon, käräjäoikeus voi määrätä tietoyhteiskunnan palvelun tarjoajan huolehtimaan tiedoksiannosta. Määräys raukeaa, jollei sen kohteena olevan tiedon sisältöön tai välittämiseen perustuvasta rikoksesta nosteta syytettä tai, milloin kysymys on korvausvastuusta, panna vireille kannetta kolmen kuukauden kuluessa määräyksen antamisesta. Käräjäoikeus voi syyttäjän, asianomistajan tai asianosaisen edellä tarkoitettuna määräaikana esittämästä	Information Society Code (917/2014), Chapter 22, section 185 Order to disable access to information Upon request from a public prosecutor or a person in charge of inquiries or on application by a party whose right the matter concerns, a court may order the information society service provider referred to in section 184 to disable access to the information stored by it if the information is clearly such that keeping its content available to the public or its transmission is prescribed punishable or as a basis for civil liability. The court shall urgently process the application. The application cannot be approved without an opportunity for the service provider and the content provider an opportunity to be consulted except if the consultation cannot be arranged as quickly as the urgency of the matter so necessarily requires. A court order must also be made known to the content provider. If the content provider is not known, the court may order the information society service provider to take care of notification. An order ceases to be in effect unless charges are raised for an offence based on the content or transmission of information referred to in the order or, when concerning a liability, action is brought within three months of issuing the order. On request by a public prosecutor, by an injured party or

vaatimuksesta pidentää tätä määräaikaa enintään kolmella kuukaudella. Tietoyhteiskunnan palvelun tarjoajalla ja sisällön tuottajalla on oikeus hakea määräyksen kumoamista siinä käräjäoikeudessa, jossa määräys on annettu. Määräyksen kumoamista koskevan asian käsittelyssä noudatetaan oikeudenkäymiskaaren 8 luvun säännöksiä. Tuomioistuin huolehtii kuitenkin tarpeellisista toimenpiteistä syyttäjän kuulemiseksi. Kumoamista on haettava 14 päivän kuluessa siitä, kun hakija on saanut tiedon määräyksestä. Tietoa ei saa saattaa uudelleen saataville kumoamista koskevan asian käsittelyn ollessa vireillä, ellei asiaa käsittelevä tuomioistuin toisin määrää. Myös syyttäjällä on oikeus hakea muutosta päätökseen, jolla määräys on kumottu.	by an interested party within the time limit referred to above, the court may extend this time limit by a maximum of three months. The information society service provider and the content provider have the right to apply for reversal of the order in the court where the order was issued. When dealing with a matter concerning reversal of the order, the provisions of Chapter 8 of the Code of Judicial Procedure shall be observed. However, the court takes care of the necessary procedures to hear a public prosecutor. The reversal must be applied for within 14 days of the date when the applicant was notified of the order. The information must not be made available again when the hearing of the case concerning the reversal is pending unless otherwise ordered by the court dealing with the case. A public prosecutor has also the right to appeal the decision that reversed the order.
Tietoyhteiskuntakaari (917/2014), Luku 22, 187 § Sisällön tuottajan oikeusturva Jos tietoyhteiskunnan palvelun tarjoaja on estänyt tiedon saannin 184 §:n 1 momentin 2 kohdan nojalla, hänen on viipymättä ilmoitettava siitä sisällön tuottajalle kirjallisesti tai sähköisesti siten, että ilmoituksen sisältöä ei voida yksipuolisesti muuttaa ja että se säilyy osapuolten saatavilla. Ilmoituksessa on mainittava eston syy sekä tieto sisällön tuottajan oikeudesta saattaa asia tuomioistuimen käsiteltäväksi. Ilmoitus on tehtävä sisällön tuottajan äidinkielellä, suomeksi tai ruotsiksi. Ilmoitus voidaan tehdä myös sisällön tuottajan kanssa sovitulla muulla kielellä. Sisällön tuottajalla on oikeus saattaa estoa koskeva asia 186 §:ssä tarkoitetun tuomioistuimen käsiteltäväksi 14 päivän kuluessa siitä, kun hän on saanut 1 momentissa tarkoitetun ilmoituksen. Estoa koskevan asian käsittelyssä noudatetaan, mitä 185 §:n 4 momentissa säädetään.	Information Society Code (917/2014), Chapter 22, section 187 Legal safeguards for the content provider If the information society service provider has prevented access to information under section 184(1)(2), it shall immediately notify the content provider of this in writing or electronically so that the content of the notification cannot be unilaterally altered and it remains accessible to the parties. The notification must state the reason for prevention as well as information on the right of the content provider to bring the matter for a court hearing. The notification must be made in the mother tongue of the content provider, in Finnish or in Swedish. The notification may also be made in another language agreed with the content provider. The content provider has the right to bring the matter concerning prevention to be heard by the court referred to in section 186 within 14 days from the receipt of the notification referred to in subsection 1. The provisions of section 185(4) shall be observed during the hearing of the case concerning prevention.
Tietoyhteiskuntakaari (917/2014), Luku 22, 189 §	Information Society Code (917/2014), Chapter 22, section 189

Tekijänoikeutta tai lähioikeutta loukkaavan aineiston saannin estäminen Tekijänoikeuden haltija tai hänen edustajansa voi vaatia 184 §:ssä tarkoitettua tietoyhteiskunnan palvelun tarjoajaa estämään tekijänoikeutta loukkaavan aineiston saannin siten kuin tässä pykälässä ja 191–193 §:ssä säädetään. Sama koskee lähioikeuden haltijaa ja hänen edustajaansa, jos kysymys on tällaista oikeutta loukkaavasta aineistosta. Vaatimus on esitettävä ensin sille sisällön tuottajalle, jonka toimittamaa aineistoa vaatimus koskee. Jos sisällön tuottajaa ei voida tunnistaa tai jos hän ei viipymättä poista aineistoa tai estä sen saantia, vaatimus voidaan tehdä tietoyhteiskunnan palvelun tarjoajalle 191 §:ssä säädetyllä ilmoituksella.	Prevention of access to material infringing copyright or neighbouring right A holder of a copyright or his/her representative may request the information society service provider referred to in section 184 to prevent access to material infringing copyright as prescribed in this section and in sections 191–193. The same applies to a holder of a neighbouring right and his/her representative if it concerns material infringing this right. A request must first be presented to the content provider whose material the request concerns. If the content provider cannot be identified or if he/she does not remove the material or prevent access to it expeditiously, the request may be submitted to the information society service provider by notification prescribed in section 191.
Tietoyhteiskuntakaari (917/2014), Luku 22, 190 § Tietoyhteiskunnan palvelun tarjoajan yhteyspiste Tietoyhteiskunnan palvelun tarjoajan on ilmoitettava yhteyspiste, jonne 191 §:ssä tarkoitettu ilmoitus ja 192 §:ssä tarkoitettu vastine voidaan toimittaa. Yhteyspisteen yhteystietojen on oltava saatavilla helposti ja jatkuvasti.	Information Society Code (917/2014), Chapter 22, section 190 Information society service provider's contact point The information society service provider shall give a contact point where the notification referred to in section 191 and the plea referred to in section 192 may be delivered. The contact information of the contact point shall be easily and continuously accessible.
Tietoyhteiskuntakaari (917/2014), Luku 22, 191 § Ilmoituksen muoto ja sisältö Edellä 189 §:ssä tarkoitetun vaatimuksen sisältävä ilmoitus on tehtävä kirjallisesti tai sähköisesti siten, että ilmoituksen sisältöä ei voida yksipuolisesti muuttaa ja että se säilyy osapuolten saatavilla. Ilmoituksessa on oltava: 1) ilmoituksen tekijän nimi ja yhteystiedot; 2) yksilöityinä se aineisto, jonka saannin estämistä vaaditaan, sekä selvitys aineiston sijainnista; 3) ilmoituksen tekijän vakuutus siitä, että se aineisto, jota vaatimus koskee, on hänen vilpittömän käsityksensä mukaan lainvastaisesti saatavilla viestintäverkossa; 4) tieto siitä, että ilmoituksen tekijä on tuloksetta esittänyt vaatimuksensa sisällön tuottajalle tai että sisällön tuottajaa ei ole voitu tunnistaa;	Information Society Code (917/2014), Chapter 22, section 191 Form and content of the notification The notification referred to in section 189 shall be made in writing or electronically so that the content of the notification cannot be unilaterally altered and it remains available to the parties. The notification shall include: 1) the name and contact information of the notifying party; 2) an itemisation of the material, for which prevention of access is requested, and details of the location of the material; 3) confirmation by the notifying party that the material which the request concerns is, in its sincere opinion, illegally accessible in the communications network; 4) information concerning the fact that the notifying party has in vain submitted its

5) ilmoituksen tekijän vakuutus siitä, että hän on tekijänoikeuden tai lähioikeuden haltija taikka oikeutettu toimimaan oikeudenhaltijan puolesta; 6) ilmoituksen tekijän allekirjoitus. Ilmoitus, joka ei täytä 1 momentissa säädettyjä vaatimuksia, on tehoton. Jos ilmoituksen puutteet koskevat yksinomaan 1 momentin 2 kohdassa tarkoitettuja tietoja, tietoyhteiskunnan palvelun tarjoajan on kuitenkin ryhdyttävä kohtuullisiin toimiin ilmoituksen tekijän tavoittamiseksi ja ilmoitettava tälle havaitsemansa puutteet.	request to the content provider or that the content provider could not be identified; 5) confirmation by the notifying party that he/she is the holder of copyright or neighbouring right or entitled to act on behalf of the holder of the right; 6) signature of the notifying party. A notification that does not meet the requirements in subsection 1 is invalid. If the shortcomings in the notification solely concern the information referred to in subsection 1(2), the information society service provider shall, however, take reasonable steps to contact the notifying party and to communicate the shortcomings discovered.
Tietoyhteiskuntakaari (917/2014), Luku 22, 192 § Ilmoitus sisällön tuottajalle ja vastine Tietoyhteiskunnan palvelun tarjoajan on viipymättä ilmoitettava sisällön tuottajalle tämän toimittaman aineiston saannin estämisestä sekä toimitettava sisällön tuottajalle jäljennös ilmoituksesta, jonka perusteella esto on tehty. Jos sisällön tuottaja katsoo eston olevan perusteeton, hän voi saada aineiston palautetuksi toimittamalla ilmoituksen tekijälle vastineen kirjallisesti tai 191 §:ssä säädetyllä tavalla sähköisesti 14 päivän kuluessa ilmoituksesta tiedon saatuaan. Jäljennös vastineesta on toimitettava palvelun tarjoajalle. Vastineessa on oltava: 1) sisällön tuottajan nimi ja yhteystiedot; 2) ne tosiseikat ja muut syyt, joiden nojalla esto katsotaan perusteettomaksi; 3) yksilöityinä se aineisto, jonka esto katsotaan perusteettomaksi; 4) sisällön tuottajan allekirjoitus.	Information Society Code (917/2014), Chapter 22, section 192 Notification to the content provider and the plea The information society service provider shall immediately notify the content provider of prevention of access to the material supplied by him/her and to supply the content provider with a copy of the notification on the basis of which prevention was made. If the content provider considers that prevention is groundless, he/she may get the material returned by delivering to the notifying party a plea in writing or electronically, as prescribed in section 191, within 14 days of receiving the notification. A copy of the plea shall be delivered to the service provider. The plea must include: 1) the name and contact information of the content provider; 2) the facts and other reasons under which prevention is considered groundless; 3) an itemisation of the material for which prevention is considered groundless; 4) signature by the content provider.
Tietoyhteiskuntakaari (917/2014), Luku 22, 193 § Aineiston palauttaminen Jos 192 §:ssä säädetyt vaatimukset täyttävä vastine on määräajassa toimitettu, tietoyhteiskunnan palvelun tarjoaja ei saa estää vastineessa yksilöidyn aineiston palauttamista ja sen pitämistä saatavilla, ellei palvelun tarjoajan ja sisällön tuottajan välisestä sopimuksesta taikka	Information Society Code (917/2014), Chapter 22, section 193 Returning the material If the plea, meeting the requirements of section 192, is delivered within the time limit, the information society service provider must not prevent the material specified in the plea from being returned and kept available unless otherwise provided by an agreement between the service

tuomioistuimen tai muun viranomaisen määräyksestä tai päätöksestä johdu muuta.	provider and the content provider or by an order or decision by a court or by any other authority.
Tietoyhteiskuntakaari (917/2014), Luku 22, 194 § Korvausvelvollisuus Joka antaa väärän tiedon 191 §:ssä tarkoitetussa ilmoituksessa tai 192 §:ssä tarkoitetussa vastineessa, on velvollinen korvaamaan siitä aiheutuvan vahingon. Korvausvelvollisuutta ei kuitenkaan ole tai sitä voidaan sovitella, jos tiedon antaneella oli ollut perusteltua aihetta olettaa tietoa oikeaksi tai jos väärällä tiedolla oli vain vähäinen merkitys ilmoituksen tai vastineen koko sisältö huomioon ottaen.	Information Society Code (917/2014), Chapter 22, section 194 Liability to compensate A person who gives false information in the notification referred to in section 191 or in the plea referred to in section 192 shall be liable to compensate for the damage caused. However, there is no liability to compensate or it may be adjusted if the notifying party had reasonable grounds to assume that the information is correct or if the false information is only of minor significance, when taking into account the entire content of the notification or the plea.
Lakivaliokunnan mietintö 39/2010	Statement of the Legal Affairs Committee 39/2010
Perustuslaki (1.6.1999/731) 10 § Yksityiselämän suoja Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. (5.10.2018/817) Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. (5.10.2018/817)	The Constitution of Finland (1.6.1999/731), section 10 - The right to privacy Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. The secrecy of correspondence, telephony and other confidential communications is inviolable. Measures encroaching on the sanctity of the home which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime may be laid down by an Act. (817/2018, entry into force 15.10.2018) Limitations of the secrecy of communications may be imposed byan Act if they are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, during deprivation of liberty, and for the purpose of obtaining information on military activities or other such activities that pose a serious threat to national security. (817/2018, entry into force 15.10.2018)
Perustuslaki (1.6.1999/731) 11 § Uskonnon ja omantunnon vapaus Jokaisella on uskonnon ja omantunnon vapaus. Uskonnon ja omantunnon vapauteen sisältyy oikeus tunnustaa ja harjoittaa uskontoa, oikeus ilmaista vakaumus ja	The Constitution of Finland (1.6.1999/731), section 11 – Freedom of religion and conscience. Everyone has the freedom of religion and conscience. Freedom of religion and conscience entails the right to profess and practice a religion,

oikeus kuulua tai olla kuulumatta uskonnolliseen yhdyskuntaan. Kukaan ei ole velvollinen osallistumaan omantuntonsa vastaisesti uskonnon harjoittamiseen.	the right to express one's convictions and the right to be a member of or decline to be a member of a religious community. No one is under the obligation, against his or her conscience to participate in the practice of religion.
Perustuslaki (1.6.1999/731) 12 § Sananvapaus ja julkisuus Jokaisella on sananvapaus. Sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Tarkempia säännöksiä sananvapauden käyttämisestä annetaan lailla. Lailla voidaan säätää kuvaohjelmia koskevia lasten suojelemiseksi välttämättömiä rajoituksia. Viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.	The Constitution of Finland (1.6.1999/731), section 12 - Freedom of expression and right of access to information Everyone has the freedom of expression. Freedom of expression entails the right to express, disseminate and receive information, opinions and other communications without prior prevention by anyone. More detailed provisions on the exercise of the freedom of expression are laid down by an Act. Provisions on restrictions relating to pictorial programmes that are necessary for the protection of children may be laid down by an Act. Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.
Perustuslaki (1.6.1999/731) 15 § Omaisuuden suoja Jokaisen omaisuus on turvattu. Omaisuuden pakkolunastuksesta yleiseen tarpeeseen täyttä korvausta vastaan säädetään lailla.	The Constitution of Finland (1.6.1999/731) Section 15 - Protection of property The property of everyone is protected. Provisions on the expropriation of property, for public needs and against full compensation, are laid down by an Act.
Rikoslaki (39/1889) Luku 17, 10 § Uskonrauhan rikkominen Joka 1) julkisesti pilkkaa Jumalaa tai loukkaamistarkoituksessa julkisesti herjaa tai häpäisee sitä, mitä uskonnonvapauslaissa (267/1922) tarkoitettu kirkko tai uskonnollinen yhdyskunta muutoin pitää pyhänä, tai 2) meluamalla, uhkaavalla käyttäytymisellään tai muuten häiritsee jumalanpalvelusta, kirkollista toimitusta, muuta sellaista uskonnonharjoitusta taikka hautaustilaisuutta, on tuomittava uskonrauhan rikkomisesta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.	The Criminal Code of Finland (39/1889), Chapter 17, Section 10 - Breach of the sanctity of religion A person who (1) publicly blasphemes against God or, for the purpose of offending, publicly defames or desecrates what is otherwise held to be sacred by a church or religious community, as referred to in the Act on the Freedom of Religion (267/1922), or (2) by making noise, acting threateningly or otherwise, disturbs worship, ecclesiastical proceedings, other similar religious proceedings or a funeral, shall be sentenced for a breach of the sanctity of religion to a fine or to imprisonment for at most six months.

Rikoslaki (39/1889) Luku 17, 18 § Sukupuolisiveellisyyttä loukkaavan kuvan levittäminen Joka valmistaa, pitää kaupan tai vuokrattavana taikka muulla tavoin tarjoaa tai asettaa saataville, pitää saatavilla, vie maasta, tuo maahan tai Suomen kautta muuhun maahan taikka muuten levittää kuvia tai kuvatallenteita, joissa sukupuolisiveellisyyttä loukkaavasti todellisuuspohjaisesti tai todenmukaisesti esitetään 1) lasta, 2) väkivaltaa tai 3) eläimeen sekaantumista, on tuomittava sukupuolisiveellisyyttä loukkaavan kuvan levittämisestä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Yritys on rangaistava. Mitä 17 §:n 2 momentissa säädetään, koskee myös tässä pykälässä tarkoitettua kuvaa tai kuvatallennetta. Lapsena pidetään kahdeksaatoista vuotta nuorempaa henkilöä sekä henkilöä, jonka ikää ei voida selvittää mutta jonka on perusteltua syytä olettaa olevan kahdeksaatoista vuotta nuorempi. Kuva tai kuvatallenne on 1 momentin 1 kohdassa tarkoitetulla tavalla todellisuuspohjainen, jos se on valmistettu tilanteesta, jossa lapsi on tosiasiallisesti ollut sukupuolisiveellisyyttä loukkaavan toiminnan kohteena, ja todenmukainen, jos se erehdyttävästi muistuttaa valokuvaamalla tai muulla vastaavalla menetelmällä valmistettua kuvaa tai kuvatallennetta tilanteesta, jossa lapsi on sukupuolisiveellisyyttä loukkaavan toiminnan kohteena. Todellisuuspohjaisen ja todenmukaisen määritelmiä sovelletaan vastaavasti 1 momentin 2 ja 3 kohdassa tarkoitetuissa tapauksissa.	The Criminal Code of Finland (39/1889), Chapter 17, Section 18 - Distribution of a sexually offensive picture (1) A person who manufactures, offers for sale or for rent or otherwise offers or makes available, keeps available, exports, imports to or transports through Finland to another country, or otherwise distributes pictures or visual recordings that factually or realistically depict (1) a child, (2) violence or (3) bestiality shall be sentenced for distribution of a sexually offensive picture to a fine or imprisonment for at most two years. (540/2011) (2) An attempt is punishable. (3) The provisions in section 17, subsection 2 apply also to the pictures and visual recordings referred to in this section. (4) A child is defined as a person below the age of eighteen years and a person whose age cannot be determined but whom there is justifiable reason to assume is below the age of eighteen years. The picture or visual recording is deemed factual in the manner referred to in subsection 1, paragraph 1, if it has been produced in a situation in which a child has actually been the object of sexually offensive conduct and realistic, if it resembles in a misleading manner a picture or a visual recording produced through photography or in another corresponding manner of a situation in which a child is the object of sexually offensive conduct. The definitions of the terms factual and realistic apply correspondingly in the cases referred to in subsection 1, paragraphs 2 and 3.
Rikoslaki (39/1889) Luku 24, 8 § Yksityiselämää loukkaava tiedon levittäminen Joka oikeudettomasti 1) joukkotiedotusvälinettä käyttämällä tai 2) muuten toimittamalla lukuisten ihmisten saataville esittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko on omiaan aiheuttamaan vahinkoa tai	The Criminal Code of Finland (39/1889), Chapter 24, Section 8 – Dissemination of information violating personal privacy (1) A person who unlawfully (1) through the use of the mass media, or (2) otherwise by making available to many persons disseminates information, an insinuation or an image of the private life of another

kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, on tuomittava yksityiselämää loukkaavasta tiedon levittämisestä sakkoon. Yksityiselämää loukkaavana tiedon levittämisenä ei pidetä sellaisen yksityiselämää koskevan tiedon, vihjauksen tai kuvan esittämistä politiikassa, elinkeinoelämässä tai julkisessa virassa tai tehtävässä taikka näihin rinnastettavassa tehtävässä toimivasta, joka voi vaikuttaa tämän toiminnan arviointiin mainitussa tehtävässä, jos esittäminen on tarpeen yhteiskunnallisesti merkittävän asian käsittelemiseksi. Yksityiselämää loukkaavana tiedon levittämisenä ei myöskään pidetä yleiseltä kannalta merkittävän asian käsittelemiseksi esitettyä ilmaisua, jos sen esittäminen, huomioon ottaen sen sisältö, toisten oikeudet ja muut olosuhteet, ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä.	person, so that the act is conducive to causing that person damage or suffering, or subjecting that person to contempt, shall be sentenced for dissemination of information violating personal privacy to a fine. (2) The spreading of information, an insinuation or an image of the private life of a person in politics, business, public office or public position, or in a comparable position, does not constitute dissemination of information violating personal privacy, if it may affect the evaluation of that person's activities in the position in question and if it is necessary for purposes of dealing with a matter of importance to society. (3) Presentation of an expression in the consideration of a matter of general importance shall also not be considered dissemination of information violating personal privacy if its presentation, taking into consideration its contents, the rights of others and the other circumstances, does not clearly exceed what can be deemed acceptable.
Arpajaislaki (1047/2001) 62 § Arpajaisten toimeenpanoa koskevat kiellot Arpajaisten toimeenpano muulla kuin 3 §:n 2 tai 3 momentissa, 3 a §:ssä taikka 56 §:ssä tarkoitetulla tavalla on kielletty. Kiellettyä on: 1) arpojen myyminen ja välittäminen ilman tässä laissa edellytettyä lupaa toimeenpantuihin arpajaisiin ja muun kuin Veikkaus Oy:n toimeenpanemaan rahapeliin sekä tällaisten arpajaisten markkinointi; 2) arpojen myyminen tai välittäminen tai arpajaisten markkinointi ulkomaille, jollei se ole sallittua sen valtion tai alueen lainsäädännön mukaan, johon arpoja myydään tai välitetään taikka arpajaisia markkinoidaan; 3) Veikkaus Oy:n toimeenpanemaan rahapeliin liittyvien arpojen myyminen, välittäminen, pelipanosten vastaanottaminen ja voittojen välittäminen ilman yhtiön lupaa. Tilan luovuttaminen ilman tässä laissa tarkoitettua lupaa tapahtuvaan raha-automaattien, erityisautomaattien, kasinopelien, tavaravoittoautomaattien tai 56 §:ssä tarkoitettujen peliautomaattien ja pelilaitteiden käytettävänä pitämiseen on kielletty.	Lotteries Act (1047/2001) Section 62 Prohibitions on running a lottery Running a lottery in a manner other than that referred to in section 3, subsection 2 or 3, or section 3a or 56 is prohibited. It is prohibited to 1) sell or supply tickets for a lottery run without a licence required under this Act, or any other gambling services than those provided by Veikkaus Oy, or market such a lottery; 2) sell or supply tickets or market lotteries abroad, unless permitted under the legislation of the state or region in which the tickets are sold or supplied or lotteries are marketed; 3) sell or supply tickets, receive stakes and distribute winnings connected with gambling services provided by Veikkaus Oy without the permission of the company it is prohibited to provide premises for the making of slot machines, specialty gaming machines, casino games, non-money prize machines, or game machines or game equipment referred to in section 56, available for use without a licence referred to in this Act.

Liikkeelle laskettavalle joukkovelkakirjalle ei saa koron lisäksi maksaa arpomiseen perustuvaa hyvitystä. Ulkomailla toimeenpantavina arpajaisina ei pidetä rahapelejä, joiden toimeenpanoon osallistuu Veikkaus Oy.	A bonus based on a draw may not be paid on premium bonds in addition to interest. Gambling services conducted abroad in which Veikkaus Oy participates are not considered overseas lotteries under this Act.
Tekijänoikeuslaki (404/1961) 60 b § Kieltokanne Tekijällä tai hänen edustajallaan on loukkauksen jatkamisen kieltämiseksi oikeus ajaa kannetta sitä vastaan, joka saattaa tekijänoikeutta loukkaavaksi väitettyä aineistoa yleisön saataviin (väitetty loukkaaja). Hyväksyessään kanteen tuomioistuimen on samalla määrättävä, että aineiston saattaminen yleisön saataviin on lopetettava. Tuomioistuin voi asettaa määräyksen tehosteeksi uhkasakon.	Copyright Act (404/1961) Section 60 b Claim for an Injunction For the purpose of prohibiting continued violation, the author or his representative has the right to take legal action against the person who makes the allegedly copyright-infringing material available to the public (alleged infringer). In allowing the action, the court of justice shall at the same time order that the making available of the material to the public must cease. The court of justice may impose a conditional fine to reinforce the order.
Tekijänoikeuslaki (404/1961) 60 c § Keskeyttämismääräys Tuomioistuin voi kieltokannetta käsitellessään tekijän tai hänen edustajansa vaatimuksesta määrätä lähettimen, palvelimen tai muun sellaisen laitteen ylläpitäjän taikka muun välittäjänä toimivan palvelun tarjoajan (välittäjä) sakon uhalla keskeyttämään tekijänoikeutta loukkaavaksi väitetyn aineiston saattamisen yleisön saataviin (keskeyttämismääräys). Keskeyttämismääräyksen antamisen edellytyksenä on, ettei määräystä voida pitää kohtuuttomana ottaen huomioon väitetyn loukkaajan, välittäjän, aineistoa vastaanottavan henkilön ja tekijänoikeudet. Määräys ei saa vaarantaa kolmannen oikeutta lähettää ja vastaanottaa viestejä. Tuomioistuimen on varattava sekä välittäjälle että väitetylle loukkaajalle tilaisuus tulla kuulluksi. Välittäjälle lausumapyyntö voidaan antaa tiedoksi postitse taikka telekopiota tai sähköpostia käyttäen. Jos määräyksen tarkoitus saattaa muutoin vaarantua, tuomioistuin voi hakijan hakemuksesta antaa määräyksen väliaikaisena varaamatta väitetylle loukkaajalle tilaisuutta tulla kuulluksi. Väliaikainen määräys on voimassa, kunnes toisin määrätään. Väitetylle loukkaajalle on väliaikaisen määräyksen antamisen jälkeen välittömästi varattava tilaisuus tulla kuulluksi. Kun väitettyä loukkaajaa on	Copyright Act (404/1961) Section 60 Discontinuation Order (1) In considering an action to seek a discontinuation order the court of justice may, upon the request of the author or his representative, order the maintainer of the transmitter, server or other device or any other service provider acting as an intermediary (intermediary) to discontinue, on threat of fine, the making of the allegedly copyright-infringing material available to the public (discontinuation order). (2) A prerequisite for issuing a discontinuation order is that the order cannot be regarded as unreasonable in view of the rights of the alleged infringer, the intermediary, the recipient of the content and the author. The order shall not prejudice the rights of a third party to send and receive messages. (3) The court of justice shall reserve an opportunity to be heard both for the intermediary and the alleged infringer. A service of a notice to the intermediary may be delivered by posting it or by using fax or electronic mail. Upon application by the applicant, the court may issue an interim discontinuation order without reserving the alleged infringer an opportunity to be heard , if deemed necessary for the purpose of the order. The interim discontinuation order shall remain in force until further notice. After the order has been issued, the alleged

kuultu, tuomioistuimen on viipymättä päätettävä, pidetäänkö määräys voimassa vai peruutetaanko se. Keskeyttämismääräystä koskeva asia käsitellään hakemusasiana noudattaen, mitä oikeudenkäymiskaaren 7 luvussa säädetään turvaamistoimen määräämisestä. Jos syytä, jonka vuoksi keskeyttämismääräys on annettu, ei enää ole, tuomioistuimen on asiaan osallisen hakemuksesta määrättävä määräys peruutettavaksi.	infringer shall be reserved an opportunity to be heard without delay. After hearing the alleged infringer, the court shall decide without delay whether it retains the order in force or cancels it. (4) The legal action on a discontinuation order shall be tried as a non-contentious civil case, in compliance with provisions on precautionary measures referred to in Chapter 7 of the Code of Judicial Procedure. (5) If the cause for the issuing of the discontinuation order ceases to exist, the court shall, upon application by a party concerned, order the order to be cancelled.
Tekijänoikeuslaki (404/1961) 60 d § Väliaikainen keskeyttämismääräys Ennen kieltokanteen nostamista tuomioistuin voi tekijän tai hänen edustajansa hakemuksesta antaa keskeyttämismääräyksen väliaikaisena, jos määräyksen antamiselle on 60 c §:ssä säädetyt edellytykset ja on ilmeistä, että tekijän oikeuksien toteutuminen muussa tapauksessa vakavasti vaarantuisi. Määräyksen antamisessa noudatetaan, mitä 60 c §:ssä säädetään. Väitetyn loukkaajan kuulemisen jälkeen tuomioistuimen on viipymättä päätettävä, pidetäänkö määräys voimassa vai peruutetaanko se. Jos asian kiireellisyys sitä välttämättä vaatii, tuomioistuin voi antaa 1 momentissa tarkoitetun väliaikaisen keskeyttämismääräyksen, vaikka väitettyä loukkaajaa ei voida tunnistaa, jos: 1) tekijänoikeutta loukkaavaksi väitettyä aineistoa saatetaan merkittävissä määrin yleisön saataviin ilman tekijän suostumusta; tai 2) on ilmeistä, että tekijän oikeuksien toteutuminen muussa tapauksessa vakavasti vaarantuisi. Hakijan on kahden kuukauden kuluessa väliaikaisen keskeyttämismääräyksen antamisesta pantava kieltokanne vireille tuomioistuimessa. Jos kieltokannetta ei sanotussa ajassa panna vireille, määräys raukeaa. Jos 2 momentissa tarkoitetussa tilanteessa väitetty loukkaaja on jäänyt tunnistamattomaksi, hakija voi hakea 60 e §:ssä tarkoitettua estomääräystä. Jos	Copyright Act (404/1961) Section 60 Interim discontinuation order (1) Before taking legal action, the court of justice may, upon application by the author or his representative, issue an interim discontinuation order, if the issuing of the order can be justified under section 60c and if it is obvious that the rights of the author would otherwise be severely prejudiced. The issuing of the order shall be governed by the provisions in section 60c. After hearing the alleged infringer, the court shall decide without delay whether it retains the order in force or cancels it. (2) If deemed necessary for the urgency of the matter, the court of justice may issue an interim discontinuation order referred to in subsection 1 even if the alleged infringer cannot be identified, if: 1) significant amounts of allegedly copyright-infringing material is made available to the public without the author's consent; or 2) it is obvious that the rights of the author would otherwise be severely prejudiced. (3) The applicant shall institute the claim for an injunction before a court of justice within two months from the issuing of the interim discontinuation order. If the legal action is not taken within said schedule, the order shall expire. (4) If the alleged infringer has not been identified in a case referred to in subsection 2, the applicant may apply for a blocking order referred to in section 60 e. If the blocking order has been applied for within the time allotted for taking legal

estomääräystä on haettu kieltokanteen nostamiselle varatun ajan kuluessa, väliaikainen määräys ei raukea.	action, the interim discontinuation order shall not expire.
Tekijänoikeuslaki (404/1961)60 e § Estomääräys Jos kieltokanteen nostaminen ei ole mahdollista sen vuoksi, että väitetty loukkaaja on tuntematon, tuomioistuin voi tekijän tai hänen edustajansa hakemuksesta määrätä välittäjän sakon uhalla estämään tekijänoikeutta loukkaavaksi väitetyn aineiston saattamisen yleisön saataviin (estomääräys). Estomääräyksen antaminen edellyttää, että tekijänoikeutta loukkaavaksi väitettyä aineistoa merkittävissä määrin saatetaan yleisön saataviin ilman tekijän suostumusta tai on ilmeistä, että tekijän oikeuksien toteutuminen muussa tapauksessa vakavasti vaarantuisi. Estomääräyksen hakijan on ilmoitettava, mitä hän on tehnyt väitetyn loukkaajan tunnistamiseksi. Estomääräyksen antamisen edellytyksenä on, ettei määräystä voida pitää kohtuuttomana ottaen huomioon väitetyn loukkaajan, välittäjän, aineistoa vastaanottavan henkilön ja tekijänoikeudet. Määräys ei saa vaarantaa kolmannen oikeutta lähettää ja vastaanottaa viestejä. Välittäjälle on varattava tilaisuus tulla kuulluksi estomääräystä koskevasta hakemuksesta. Estomääräys annetaan määräajaksi, kuitenkin enintään vuodeksi kerrallaan. Estomääräyksen voimassaoloa voidaan hakemuksesta jatkaa, jos siihen on perusteltu syy. Jos syytä, jonka vuoksi estomääräys on annettu, ei enää ole, tuomioistuimen on asiaan osallisen hakemuksesta määrättävä määräys peruutettavaksi.	Copyright Act (404/1961) Section 60 e Blocking Order (1) If a claim for an injunction cannot be filed because the alleged infringer is unknown, the court of justice may, upon application by the author or his representative, order the intermediary to block, on threat of fine, the making of the allegedly copyright-infringing material available to the public (blocking order). The issuing of the blocking order requires that significant amounts of the allegedly copyright-infringing material are made available to the public without the author's consent or that it is obvious that the rights of the author would otherwise be severely prejudiced. (2) The applicant of the blocking order shall indicate the measures he has taken to identify the alleged infringer. (3) A prerequisite for issuing a blocking order is that the order cannot be regarded as unreasonable in view of the rights of the alleged infringer, the intermediary, the recipient of the content and the author. The order shall not prejudice the rights of a third party to send and receive messages. The intermediary shall be reserved an opportunity to be heard regarding the application for a blocking order. (4) The blocking order is issued for a fixed period, for a maximum of one year at a time. The validity of the blocking order may be extended by application for a well-founded reason. If the cause for the issuing of the blocking order ceases to exist, the court shall, upon application by a party concerned, order the blocking order to be cancelled.
Patenttilaki (550/1967)57 b § Tuomioistuin voi 57 §:n 1 momentissa tarkoitettua kannetta käsitellessään patentinhaltijan vaatimuksesta määrätä lähettimen, palvelimen tai muun sellaisen laitteen ylläpitäjän taikka muun välittäjänä toimivan palvelun tarjoajan sakon uhalla keskeyttämään patenttia loukkaavaksi väitetyn käytön (keskeyttämismääräys), jollei sitä voida pitää kohtuuttomana ottaen	Patents Act (550/1967)Section 57 b When hearing an action referred to in section 57(1) the court may at the patent holder's request prohibit the keeper of a transmitter, server or other similar device or other service provider acting as an intermediary, under penalty of a fine, from continuing the use alleged to infringe the patent (injunction order) unless it can be considered disproportionate in view of the rights of the alleged infringer of the patent

huomioon patentin väitetyn loukkaajan, välittäjän ja patentinhaltijan oikeudet.	or in view of the rights of the intermediary or patent holder. (21.7.2006/684)
Ennen 57 §:n 1 momentissa tarkoitetun kanteen nostamista tuomioistuin voi patentinhaltijan hakemuksesta antaa keskeyttämismääräyksen, jos sen antamiselle on 1 momentissa mainitut edellytykset ja jos on ilmeistä, että patentinhaltijan oikeuksien toteutuminen muutoin vakavasti vaarantuisi. Tuomioistuimen on varattava sekä sille, jolle määräystä on haettu annettavaksi, että sille, jonka väitetään loukkaavan patenttia, tilaisuus tulla kuulluksi. Tiedoksianto sille, jolle määräystä on haettu annettavaksi, voidaan toimittaa postitse taikka telekopiota tai sähköpostia käyttäen. (31.1.2013/101)	Before the bringing of an action referred to in section 57(1), the court may, at the patent proprietor's request, issue an injunction if the preconditions for it set out in subsection 1 exist and if it is obvious that the patent proprietor's rights otherwise would be seriously endangered. The court must provide both for the party against whom the injunction is sought and for the party who is claimed to infringe the patent an opportunity to be heard. Communications to the party against whom the injunction has been sought may be delivered by mail, facsimile or email. (31.1.2013/101)
Tuomioistuin voi pyynnöstä antaa 2 momentissa tarkoitetun keskeyttämismääräyksen väliaikaisena väitettyä loukkaajaa kuulematta, jos asian kiireellisyys sitä välttämättä vaatii. Määräys on voimassa, kunnes toisin määrätään. Väitetylle loukkaajalle on määräyksen antamisen jälkeen viipymättä varattava tilaisuus tulla kuulluksi. Kun väitettyä loukkaajaa on kuultu, tuomioistuimen on viipymättä päätettävä, pidetäänkö määräys voimassa vai peruutetaanko se.	The court may, on request, issue the injunction referred to in subsection (2) as an interlocutory injunction without hearing the alleged infringer, if the urgency of the case of necessity requires that. The injunction remains in force until ordered otherwise. After the injunction is issued, the alleged infringer must without delay be provided an opportunity to be heard. When the alleged infringer has been heard, the court must decide without delay whether to keep the injunction in force or withdraw it. (21.7.2006/684)
Tämän pykälän nojalla annettu keskeyttämismääräys ei saa vaarantaa kolmannen oikeutta lähettää ja vastaanottaa viestejä. Keskeyttämismääräys tulee voimaan, kun hakija asettaa ulosottomiehelle ulosottokaaren (705/2007) 8 luvun 2 §:ssä tarkoitetun vakuuden. Mahdollisuudesta vapautua vakuuden asettamisesta säädetään oikeudenkäymiskaaren 7 luvun 7 §:ssä.	An injunction issued under this section must not endanger the right of a third party to send and receive messages. The injunction comes into force when the applicant lodges with the bailiff security referred to in Chapter 8, section 2, of the Enforcement Code (705/2007). The provisions of Chapter 7, section 7, of the Code of Judicial Procedure apply to the possibility to be released from lodging security. An injunction issued under subsection (2) or (3) above lapses if the action referred to in section 57(1) is not brought before a court within a month from the issuance of the injunction. (31.1.2013/101)
Edellä 2 tai 3 momentin nojalla annettu keskeyttämismääräys raukeaa, jollei 57 §:n 1 momentissa tarkoitettua kannetta nosteta tuomioistuimessa kuukauden kuluessa määräyksen antamisesta. (31.1.2013/101)	
Keskeyttämismääräystä vaatineen on korvattava sille, jolle määräys on annettu, samoin kuin väitetylle loukkaajalle määräyksen täytäntöönpanosta aiheutunut vahinko sekä asiassa aiheutuneet kulut, jos 57 §:n 1 momentissa tarkoitettu kanne hylätään tai jätetään tutkimatta taikka jos asian käsittely jätetään sillensä sen vuoksi, että kantaja on peruuttanut kanteensa tai jäänyt saapumatta tuomioistuimeen. Sama	The party who has demanded the injunction must compensate the party against whom the injunction is issued as well as the alleged infringer for the damage caused by the implementation of the injunction and for any other costs resulting from the case if the action referred to in section 57(1) is rejected

on voimassa, jos keskeyttämismääräys 3 momentin nojalla peruutetaan tai 4 momentin nojalla raukeaa. Vahingon ja kulujen korvaamista koskevan kanteen nostamisessa noudatetaan, mitä oikeudenkäymiskaaren 7 luvun 12 §:ssä säädetään.	or ruled inadmissible, or if the processing of the case is removed from the cause list because the plaintiff has abandoned his/her action or failed to arrive to the court. The same applies if the injunction is withdrawn under subsection (3) or lapses under subsection (4). When an action is brought for compensation for damage and costs, the provisions of Chapter 7, section 12, of the Code of Judicial Procedure apply. (21.7.2006/684)
Sananvapauslaki (460/2003) 16 § Lähdesuoja ja oikeus anonyymiin ilmaisuun. Yleisön saataville toimitetun viestin laatijalla sekä julkaisijalla ja ohjelmatoiminnan harjoittajalla on oikeus olla ilmaisematta, kuka on antanut viestin sisältämät tiedot. Julkaisijalla ja ohjelmatoiminnan harjoittajalla on lisäksi oikeus olla ilmaisematta viestin laatijan henkilöllisyyttä. Edellä 1 momentissa tarkoitettu oikeus on myös sillä, joka on saanut mainituista seikoista tiedon ollessaan viestin laatijan taikka julkaisijan tai ohjelmatoiminnan harjoittajan palveluksessa. Velvollisuudesta ilmaista 1 momentissa tarkoitettu tieto esitutkinnassa tai oikeudenkäynnissä säädetään erikseen.	Act on the Exercise of Freedom of Expression in Mass Media (460/2003) Section 16 Source protection and the right to anonymous expression. The author of the message made available to the public, as well as the publisher and the program operator, have the right not to disclose who has provided the information contained in the message. In addition, the publisher and the program operator have the right not to disclose the identity of the author of the message. The right referred to in subsection 1 above also belongs to the person who has received information about the said facts while being employed by the author of the message or the publisher or program operator. The obligation to disclose the information referred to in subsection 1 in a preliminary investigation or trial is provided separately.
Sananvapauslaki (460/2003) 18 § Verkkoviestin jakelun keskeyttämismääräys Tuomioistuin voi virallisen syyttäjän, tutkinnanjohtajan tai asianomistajan hakemuksesta määrätä julkaisijan tai ohjelmatoiminnan harjoittajan taikka lähettimen, palvelimen tai muun sellaisen laitteen ylläpitäjän keskeyttämään julkaistun verkkoviestin jakelun, jos viestin sisällön perusteella on ilmeistä, että sen pitäminen yleisön saatavilla on säädetty rangaistavaksi. Tuomioistuimen on käsiteltävä hakemus kiireellisenä. Ennen määräyksen antamista tuomioistuimen on varattava sille, jolle määräystä on haettu annettavaksi, ja verkkoviestin lähettäjälle tilaisuus tulla kuulluksi, jollei asian kiireellisyys välttämättä muuta vaadi. Tuomioistuimen määräys on annettava tiedoksi myös siinä tarkoitetun verkkoviestin	Act on the Exercise of Freedom of Expression in Mass Media (460/2003) Section 18 Order to cease the distribution of a network message On the request of the public prosecutor, the head of a pre-trial investigation, or the injured party, a court may order that the publisher, broadcaster or keeper of a transmitter, server or other comparable device is to cease the distribution of a published network message, if it is evident on the basis of the contents of the message that providing it to the public is a criminal offence. The court shall deal with the request as a matter of urgency. Before issuing a cease order, the court shall reserve the intended addressee of the order and the sender of the network message an opportunity to be heard, unless the urgency

lähettäjälle. Jos lähettäjä on tuntematon, tuomioistuin voi määrätä lähettimen, palvelimen tai muun sellaisen laitteen ylläpitäjän huolehtimaan tiedoksiannosta. Edellä 1 momentissa tarkoitettu määräys raukeaa, jollei kolmen kuukauden kuluessa sen antamisesta nosteta syytettä määräyksen kohteena olevan viestin sisältöön perustuvasta rikoksesta, esitetä 22 §:ssä tarkoitettua vaatimusta tai nosteta kannetta viestin sisällöstä aiheutuneen vahingon korvaamisesta. Tuomioistuin voi virallisen syyttäjän tai asianomistajan edellä tarkoitettuna määräaikana esittämästä vaatimuksesta pidentää tätä määräaikaa enintään kolmella kuukaudella. Sillä, jolle on annettu määräys keskeyttää verkkoviestin pitäminen yleisön saatavilla, samoin kuin verkkoviestin lähettäjällä on oikeus hakea keskeyttämismääräyksen kumoamista siinä tuomioistuimessa, jossa määräys on annettu. Määräyksen kumoamista koskevan asian käsittelyssä noudatetaan, mitä oikeudenkäymiskaaren 8 luvussa säädetään. Tuomioistuin huolehtii kuitenkin tarpeellisista toimenpiteistä virallisen syyttäjän kuulemiseksi. Kumoamista on haettava 14 päivän kuluessa siitä, kun hakija on saanut tiedon määräyksestä. Verkkoviestiä ei saa saattaa uudelleen yleisön saataville kumoamista koskevan asian käsittelyn ollessa vireillä, ellei asiaa käsittelevä tuomioistuin toisin määrää. Myös virallisella syyttäjällä on oikeus hakea muutosta päätökseen, jolla määräys on kumottu. Tuomioistuin voi virallisen syyttäjän tai asianomistajan vaatimuksesta antaa 1 momentissa tarkoitetun määräyksen myös käsitellessään julkaistun viestin sisältöön perustuvaa syytettä, vaatimusta 22 §:n mukaisen seuraamuksen määräämisestä tai kannetta viestin sisällöstä aiheutuneen vahingon korvaamisesta. Tässä tarkoitettuun määräykseen ei saa hakea erikseen muutosta valittamalla.	of the matter otherwise necessitates. Notice of the cease order shall be served also on the sender of the network message referred to therein. If the sender is unknown, the court may order that the keeper of the transmitter, server or other comparable device sees to the service. A cease order referred to in subsection (1) shall lapse, unless within three months of its issue a charge is brought for an offence arising from the contents of the relevant message, or a demand referred to in section 22 is made, or a tort action pertaining to the contents of the message is brought. On the request of the public prosecutor or the injured party, submitted before the deadline referred to above, the court may extend that deadline by three months at the most. The person who has been issued with a cease order, as well as the sender of the network message, have the right to apply for the reversal of the cease order from the court that originally issued it. The provisions of chapter 8 of the Code of Judicial Procedure apply to the proceedings for the reversal of a cease order. However, the court shall take the necessary measures to hear the public prosecutor in the case. The application for a reversal shall be filed within fourteen days of the service of notice of the cease order. The network message shall not again be provided to the public while the reversal proceedings are pending, unless the court seised of the matter otherwise orders. Also the public prosecutor has standing to appeal against the reversal of a cease order. On the request of the public prosecutor or an injured party, the court may issue a cease order referred to in subsection (1) also when it is hearing charges based on the contents of a published message, a demand for a sanction referred to in section 22, or a tort action pertaining to the contents of the message. A cease order under this subsection shall not be open to appeal as a separate matter.
Laki lapsipornografian levittämisen estotoimista (1068/2006) 3 § Teleyrityksen oikeus päättää tarjoamistaan palveluista	Act on preventive measures for spreading child pornography (1068/2006) Section 3 Telecompanys right to decide the services it offers

Teleyrityksellä on oikeus tarjota palvelujaan siten, että niiden avulla ei ole pääsyä lapsipornosivustoihin.	A telecompany has a right to provide its services without offering an access to child pornography sites.
kumottu Henkilötietolaki (523/1999) 9 § Tietojen laatua koskevat periaatteet. Käsiteltävien henkilötietojen tulee olla määritellyn henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia (*tarpeellisuusvaatimus).*Rekisterinpitäjän on huolehdittava siitä, ettei virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja käsitellä (*virheettömyysvaatimus*). Rekisterinpitäjän velvollisuutta arvioitaessa on otettava huomioon henkilötietojen käsittelyn tarkoitus sekä käsittelyn merkitys rekisteröidyn yksityisyyden suojalle.	repealed Personal Data Act (523/1999) Section 9 Data quality principles The personal data processed must be necessary for the intended purpose of the processing of personal data (necessity requirement). In assessing the duty of the controller, the purpose of the processing of personal data and the importance of the processing for the protection of the data subject's privacy must be taken into account.

Bibliography

English titles

Legislation

European Convention on Human Rights [Euroopan ihmisoikeussopimus]

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Reports

Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content. Council of Europe 2015.

Recommendation No. R (97) 20 Of the Committee of Ministers to Member States On 'Hate Speech'

The European Commission against Racism and Intolerance, ECRI Report on Finland (fifth monitoring cycle)(2019),
<https://rm.coe.int/fifth-report-on-finland/1680972fa7> accessed 29 March 2020.

Weber A, Manual on Hate Speech (Council of Europe Publishing 2009)

Digital resources

Principles for a human-centric, thriving and balanced data economy. EU2019.fi. <https://api.hankeikkuna.fi/asiakirjat/2d0f4123-e651-4874-960d-5cc3fac319b6/1f6b3855-fc1d-4ea6-8636-0b8d4a1d6519/RAPORTTI_20191123084411.pdf.>, accessed 19 February 2020.

European Commission. The EU Code of conduct on countering illegal hate speechonline
<https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en>, accessed 18 March 2020.

European Data Protection Board. GDPR: Guidelines, Recommendations, Best Practices,
<https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.>, accessed 21 February 2020.

Case law

Joined Cases C-92/09 Schecke and C-93/09 Eifert [2010] ECR I-11063

Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317

Case C-324/09 L'Oréal and Others [2011] ECR I-06011 EU:C:2011:474

Korkein oikeus 2018:51

Korkein oikeus 2019:81

M.P. v. Finland App no 36487/12 (ECtHR, 15 March 2017)

Pentikäinen v. Finland App no 11882/10 (ECtHR, 20 October 2015)

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland App no 931/13 (ECtHR, 21 July 2015)

Niskasaari and Otavamedia Oy v. Finland App no 32297/10 (ECtHR, 25 June 2015)

Salumäki v. Finland App no 23605/09 (ECtHR, 29 April 2014)

Ristamäki and Korvola v. Finland App no 66456/09 (ECtHR, 29 January 2014)

Ruusunen v. Finland App no 73579/10 (ECtHR, 14 January 2014)

Ojala and Etukeno Oy v. Finland App no 68839/10 (ECtHR, 14 January 2014)

Reinboth and Others v. Finland App no 30865/08 (ECtHR, 25 April 2011)

Lahtonen v. Finland App no 29576/09 (ECtHR, 17 April 2012)

Axel Springer Ag v. Germany Appl. no. 39954/08 (ECtHR 7 February 2012)

Saaristo and Others v. Finland App no 184/06 (ECtHR, 12 January 2011)

Niskasaari and Others v. Finland App no 37520/07 (ECtHR, 6 October 2010)

Maripori v. Finland App no 37751/07 (ECtHR, 6 October 2010)

Flinkkilä v. Finland App no 25576/04 (ECtHR, 6 July 2010)

Jokitaipale and Others v. Finland App no 3349/05 (ECtHR, 6 July 2010)

Iltalehti and Karhuvaara v. Finland App no 6372/06 (ECtHR, 6 July 2010)

Soila v. Finland App no 25711/04 (ECtHR, 6 July 2010)

Tuomela and Others v. Finland App no 25711/04 (ECtHR, 6 July 2010)

Eerikäinen and Others v. Finland App no 3514/02 (ECtHR, 13 March 2009)

Hachette Filipacchi Presse Automobile and Paul Dupuy v. France (ECtHR, 5 March 2009)

Juppala v. Finland App no 18620/03 (ECtHR, 2 March 2009)

Goussev and Marek v. Finland App no 35083/97 (ECtHR, 17 April 2006)

Soini and Others v. Finland App no 36404/97 (ECtHR, 17 April 2006)

Selistö v. Finland App no 56767/00 (ECtHR, 16 February 2005)

Karhuvaara and Iltalehti v. Finland App no 53678/00 (ECtHR, 16 February 2005)

Sidabras and DŽiautas v. Lithuania Appl. nos. 55480/00 and 59330/00 (ECtHR 27 July 2004

Nikula v. Finland App no 31611/96 (ECtHR, 21 June 2002)

Finnish titles

Legislation

Arpajaislaki (1047/2001) [Lotteries Act]

Patenttilaki (550/1967) [Patents Act]

Perustuslaki 731/1999 [Constitution of Finland]

Rikoslaki (39/1889) [Penal Code]

Sananvapauslaki (460/2003) [Act on the Exercise of Freedom of Expression in Mass Media]

Tavaramerkkilaki (544/2019) [Trademark Act]

Tekijänoikeuslaki (404/1961) [Copyright Act]

Tietoyhteiskuntakaari (917/2014) [Information Society Code]

Tietosuojalaki (1050/2018) [Data Protection Act]

Lakivaliokunnan mietintö LaVM 39/2010 vp. [Statement of the Legal Affairs Committee]

Laki sähköisen viestinnän palveluista (917/2014) [Information Society Code]

Laki rikoslain muuttamisesta (511/2011) [Amendment of the Criminal Code]

Laki lapsipornografian levittämisen estotoimista (1068/2006) [Act on Preventive Measures for Spreading Child Pornography]

Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, HE 9/2018 vp. [Government Proposal to Parliament for Legislation Supplementing the European Union General Data Protection Regulation]

Hallituksen esitys Eduskunnalle laiksi tekijänoikeuslain muuttamiseksi, HE 181/2014 vp. [Government Proposal to amend the Copyright Act]

Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lisäpöytäkirjan, joka koskee tietojärjestelmien välityksellä tehtyjen luonteeltaan rasististen ja muukalaisvihamielisten tekojen kriminalisointia, hyväksymisestä ja laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain ja tietoyhteiskunnan palvelujen tarjoamisesta annetun lain 15 §:n muuttamisesta, HE 317/2010 vp. [Government Proposal to Parliament for Approval of the Additional Protocol to the Convention on Cybercrime of the Council of Europe on the Criminalization of Racist and Xenophobic Offenses Through Information Systems and the Law on the Provision of Criminal Law and Information Society Services 15]

Hallituksen esitys Eduskunnalle laiksi lapsipornografian levittämisen estotoimista, HE 99/2006 vp. [Government Proposal for Act on Preventive Measures for Spreading Child Pornography]

Perustuslakivaliokunnan mietintö 15/2002 vp, PeVM 14/2002 vp

TK 60/2019 vp

PTK 71/2019 vp

LA 30/2019 vp

Lakialoite LA 33/2019 vp

Reports

Asperlund, Sofia; Kummoinen, Katri, Kuluttajaviranomaisen toimivaltuuksien uudistaminen (Työryhmän mietintö, oikeusministeriö 2019) <http://urn.fi/URN:ISBN:978-952-259-771-7>.

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) loppumietintö. Oikeusministeriö. Mietintöjä ja lausuntoja. 8/2018. Helsinki. 2018.

Olli Pitkänen. (toim.) Tietosuojasäädösten muutostarve. Valtioneuvoston selvitys- ja tutkimustoiminta. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017.

Mäkinen K, Sanat ovat tekoja: Vihapuheen ja nettikiusaamisen vastaisten toimien tehostaminen (Sisäministeriön julkaisuja 2019:23) <http://urn.fi/URN:ISBN:978-952-324-264-7>.

Rydman, Elina, Tukia, Jukka, Rahapelilainsäädäntöä koskeva esiselvitys (Sisäministeriön julkaisuja 2019:25) http://urn.fi/URN:ISBN:978-952-324-266-1.

The Finnish Government, Programme of Prime Minister Sanna Marin's Government 10 December 2019. Inclusive and competent Finland - a socially, economically and ecologically sustainable society (Valtioneuvoston julkaisuja 2019:31), <http://urn.fi/URN:ISBN:978-952-287-808-3>.

Rauta J, Poliisin tietoon tullut viharikollisuus Suomessa 2018 (Poliisiammattikorkeakoulun raportteja, Poliisiammattikorkeakoulu 2019) <http://urn.fi/URN:NBN:fi-fe2019102935508>.

Books

Aarnio, A, Laintulkinnan teoria. (WSOY, 1989)

Haara P, Pöyhtäri R and Raittila P, Vihapuhe sananvapautta kaventamassa. (Tampere University Press 2013)

Neuvonen R (ed.), Vihapuhe Suomessa (Edita Publishing Oy 2015).

Neuvonen, Riku. Viestintäoikeuden perusteet. Helsinki. (Talentum Media 2008)

Nuotio K, Vihapuheen rikosoikeudellinen sääntelyä in book Neuvonen R (ed.), Vihapuhe Suomessa (Edita Publishing oy 2015).

Pöyhtäri R, Vihapuhe Suomessa (Edita Publishing Oy 2015)

Stromer-Galley J and Wichowski A, Political Discussion Online, The Handbook of Internet Studies (2011 Blackwell Publishing Ltd)

Periodicals

Marko Forss. Rangaistava vihapuhe Internetissä- Miten kansanryhmän suoja eroaa yksilön suojasta? [2018] 23 Edilex-sarja <https://www.edilex.fi/artikkelit/18864> accessed 1 March 2020.

Subhadeep Sarkar, Jean-Pierre Banatre, Louis Rilling and Christine Morin, 'Towards Enforcement of the EU GDPR: Enabling Data Erasure' (IEEE Conference Publications on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, Halifax, Canada, 2018)

Pekka Savola. Tekijänoikeus Internetissä - suojaamisen keinot ja strategiat. (2013) Oikeus 1/2013 (42) 1, 49-70.

Päivi Korpisaari. 'Sananvapaus verkossa - yksilöön kohdistuva vihapuhe ja verkkoalustan ylläpitäjän vastuu' (2019) 117 Lakimies 928.

Päivi Korpisaari. Henkilötietojen ja yksityiselämän suoja vuonna 2018 - Katsaus sääntelyyn ja ratkaisukäytäntöön

Tapio Lappi-Seppälä. 'Penal Policy in Scandinavia' (2007) 36(1) Crime and Justice, A Review of Research, The University of Chicago Press Journals

Kimmo Nuotio. 'Reason for Maintaining the Diversity' (2003) 6 L´Harmonisation des sanctions pénales en Europe. Delmas-Marty, M (edit.). Société de Legislation Compare.

Anu Talus. 'Tietosuojasääntelyn Eurooppalaistuminen - It is an evolution, not a revolution' Defensor Legis 2/2019

Digital resources

Ministry of Justice. Facts Against Hate,
<https://oikeusministerio.fi/hanke?tunnus=OM043:00/2019>, accessed 13 February 2020.

Teemu Lehtisaari. Internet-verkon viranomaisvalvonta ja sensuuri 2010, s. 30.

Päivi Räsäsen kirjoituksesta aloitetaan esitutkinta – Epäillään kiihottamisesta kansanryhmää vastaan YLE 4.11.2019 https://yle.fi/uutiset/3-11050903

Päivi Räsänen: Poliisi kuulusteli lähes neljä tuntia 'kristillisen uskon käsitteistä' 25 February 2020 Iltalehti https://www.iltalehti.fi/politiikka/a/8fdc58bc-7770-43c3-bc35-402246f0ea68

Rytinki, Markus: Internetsensuuri Suomessa - Sensuurin aiheet, sensuuriin liittyvät lait ja lakien valvonnan käytäntö 2014
https://www.kaleva.fi/uutiset/kotimaa/vahemmistovaltuutettu-haluaa-nettirasistit-oikeuteen/50931/

https://www.uusisuomi.fi/uutiset/nettirasistit-halutaan-kuriin-lakimuutoksia-voi-tulla/a73c40b0-b546-34b2-881b-9dc1a006bc54

https://yle.fi/uutiset/3-6113373

https://www.verkkouutiset.fi/sananvapaus-suomessa-on-uhattuna/

Hommaforum, Codex Hommaforum,
<https://cms.hommaforum.org/index.php/homman-nimi/saannot>
accessed 29 February 2020

Iltasanomat, Astrid Thorsin uhkaajalle 640 euron sakot
< https://www.is.fi/kotimaa/art-2000000362004.html> accessed 1 March 2020

Jodel, Terms of Use, part 14 < https://jodel.com/terms/> accessed 29 February 2020
Kansanedustaja Kari Tolvasen kommentti. Täysistunto session 27.11. 2019. Kohta 19.49. Muistio PTK 71/ 2019 vp.
https://www.eduskunta.fi/FI/vaski/PoytakirjaAsiakohta/Sivut/PTK_71+2019+16.aspx. Accessed 19 February 2020. Accessed 19 February 2020.

Säännöt. Ylilauta.org. https://ylilauta.org/?saannot. Accessed 12 February 2020

Kauppias latasi videon alaikäisestä 'juoksujuoman hakijasta' kauppansa Facebook-sivuille - tuomio tuli, kauppias joutuu maksamaan teinipojalle 1 500 euron korvaukset. https://www.iltalehti.fi/kotimaa/a/201807192201083983. Accessed 19 May 2020.

Mieti, mitä julkaiset sosiaalisessa mediassa - älä syyllisty rikokseen! Poliisi. https://www.poliisi.fi/sisa-suomi/tiedotteet/1/0/mieti_mita_julkaiset_sosiaalisessa_mediassa_-_ala_syyllisty_rikokseen_88098. Accessed 24 February 2020.

Jaakko Hyry, Kanter TNS Oy. Digitaalisten palveluiden käyttö - Kyselytutkimus neljässä maassa. Kokonaisraportti. Sitra. https://media.sitra.fi/2019/01/16140515/digitaaliset-palvelut-kyselytutkimus-neljassa-maassa.pdf. Accessed 28 January 2020.

Jukka Lång ja Tuomas Haavisto. Mitä muutoksia uusi kansallinen Tietosuojalaki tuo käytännössä? Edilex 2019/2. < https://www.edilex.fi/artikkelit/19271.pdf > accessed 15 January 2020.

Tuomas I. Lehtonen. Tietosuojalainsäädäntö ja julkisuusperiaate törmäävät vastakkain. Lakimiesuutiset. 18.2.2020. <https://lakimiesuutiset.fi/tietosuojalainsaadanto-ja-julkisuusperiaate-tormaavat-vastakkain/> accessed 21 February 2020

YLE Uutiset: Vihapuhe ja häirintä kaventavat sananvapautta Suomessa – sananvapauden tila on vaihdellut suuresti itsenäisyyden aikana 2019. https://yle.fi/uutiset/3-10764607

IHAN project: Fair Data Economy <https://www.sitra.fi/en/topics/fair-data-economy/>. Accessed 28 February 2020.

Case law

KHO 2018:68 [Administrative Supreme Court]

KHO 2018:12 [Administrative Supreme Court]

KHO 2013:136 [Administrative Supreme Court]

KKO 2012:58 [Supreme Court]

KKO 2010:39 [Supreme Court]

Markkinaoikeus, MAO 311:18 [Market Court]

Markkinaoikeus, MAO 243:16 [Market Court]

Helsingin hovioikeus 15.6.2012. S 11/3097 [Helsinki Court of Appeal]

Helsingin hovioikeus 15.4.2011 [Helsinki Court of Appeal]

Helsingin hallinto-oikeus 2.5.2011 [Helsinki Administrative Court]

Kouvolan hovioikeus 12.12.2011. 1146 [Kouvola Court of Appeal]

Helsingin käräjäoikeus 8.11.2017. L 16/3002 [Helsinki District Court]

Helsingin käräjäoikeus 28.6.2012. H 11/48307 [Helsinki District Court]

Helsingin käräjäoikeus 28.6.2012. H 11/51554 [Helsinki District Court]

Tietosuojavaltuutettu Docket no 637/533/2018, 28.9.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 1379/533/2018, 27.9.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 2524/533/2015, 27.8.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 85/533/2015, 25.9.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 2328/533/2016, 12.9.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 1504/533/2017, 7.9.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 1967/533/2017, 27.8.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 1973/533/2014, 31.7.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 866/533/2016, 13.7.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 3668/533/2017, 12.7.2018 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 2009/533/2014, 21.12.2016 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 3190/533/2014, 19.2.2016 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 2024/533/2014, 5.1.2016 [Data Protection Ombudsman]

Tietosuojavaltuutettu Docket no 1374/533/2015, 3.12.2015 [Data Protection Ombudsman]

ELSA France

Contributors

National Coordinator

Maja Rajić

National Academic Coordinator

Maja Rajić

National Researchers

Kilian Racon

Andrea Serfati

Marie Coustau-Guilhou

Lorenca Bejko

National Linguistic Editor

Celina Rahmoune

National Academic Supervisors

Anne-Claire Loup, Master student at University of Strasbourg

Nessan Akemakou, University Toulouse Capitole

Introduction

The topic of internet censorship has been very discussed on in France in the past couple of years, especially after the terrorist attack on the office of the satirical magazine Charlie Hebdo. Since this incident in winter 2015, French government has undertaken various measures for preventing something known as 'apology for terrorism'. Additionally, it seems interesting to further analyse how new European legislation such as General Data Protection Regulation (GDPR) has influenced domestic legislation and to speculate about its future development.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

The question of freedom of speech is an issue of central importance. Even if based in the United States and in the same way as so many other institutions, individuals and organisations all over the world, authors from the Library of Congress also attach paramount importance to the study of the extent in which this fundamental principle is today respected. The article about 'Limits on Freedom of Expression' starts by delivering a relatively meaningful analysis about the conditions in which freedom of speech can be expressed in France.

Clearly, the issue of a proper articulation between freedom of speech and the role and limitations set down by law does not seem to care about borders rather like the story exported by Rosa Parks or the so well- known Statue of Liberty.

Considered as an 'essential freedom' in France, confirmed as a constitutional right as well, Freedom of expression is protected by the Declaration of the Rights of the Man and of the Citizen of 1789. This right is also protected by the European Convention on Human Rights, Convention signed by France.[576] In a globalisation context, which leads to a considerable explosion of the flow of information, restrictions to freedom of expression are in all likelihood more often listed, which raises the question of the protection of a right inseparable from the concept of democracy.

Articles 10 and 11 of the Declaration of the Rights of the Man and the Citizen from the 26 August 1789 protect freedoms of opinion and expression. It

[576] Nicolas Boring, 'Limits on Freedom of Expression: France' (*Library of Congress,* June 2019), <https://www.loc.gov/law/help/freedom-expression/france.php> accessed 29 July 2020

describes the 'free communication of ideas and of opinions' as 'one of the most precious Rights of the Man'.

To briefly introduce these Articles, Article 10 declares that 'No one shall be disquieted on account of his opinions, including his religious views, provided their manifestation does not disturb the public order established by law.' Article 11 states that 'The free communication of ideas and opinions is one of the most precious of the Rights of the Man. Every citizen may, accordingly, speak, write, and print freely, but shall be responsible for such violations of this freedom as shall be defined by law.'

Immediately, we can note the proximity with the United States Bill of Rights which provides in its first Amendment that 'the Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.' The Assembly of freedoms until then essentially distinctly contained in different texts led, as Professor Michel Verpeaux reminds us in the 'Nouveaux cahiers du Conseil Constitutionnel N° 36 - (Dossier: La liberté d'expression et de communication, June 2012) - the French revolutionaries to gather them under the notion of freedom of communication. Additionally, still with regard to the constitutional aspect, the Constitutional revision of 23 July 2008 added to the Article 4 that the law 'guarantees the pluralistic expression of opinions.'

Very often quoted, the Law of the 29 July 1881, on Freedom of the Press enshrines the freedom of press, 'while also setting limits to what can legally be published.' Today and since this law came into force, in matters of expression, freedom is the principle and criminal treatment its exception. Press offences are judged mainly by specialised court sections, such as the 17th Chamber in Paris, considered being 'the Press Chamber.' Catherine Berlaud, in 'La Gazette du Palais' (5 November 2019), reminds us in essence that the requirement of proportionality involves ascertaining whether, having regard to the particular circumstances of the case, the publication at issue exceeds the permissible limits of freedom of expression. If those limits are not exceeded, and even if the insult is characterised in all its constituent elements, the facts which are the subject of the proceedings cannot give rise to civil damages.[577] This shows the extent to which the freedom of expression has been at the centre of public attention since the attacks on the magazine Charlie Hebdo (which happened on 7 January 2015) can be relatively broadly interpreted - in a country where, in 1958, it was still

[577] Cass. ass. plen., 25 October 2019, Nº 17-86.605

possible to be sent in front of the Court on the official grounds of 'damage to the morale of the army.'

Article 11 of the Declaration of the Rights of Man and the Citizen is therefore, in principle, widely expressed. Especially since it is supported by Article 19 of the Universal Declaration of Human Rights of 1948, which states that 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.'

Even if it must be reconciled with the notion of freedom of conscience, it may be remembered that in France - unlike in other States - the offence of blasphemy does not exist. Article 1 of the Law on the Separation of Church and State from 1905 can also be seen as providing additional support for the defence of this concept since it provides that 'the Republic shall ensure freedom of conscience. It guarantees the free exercise of worship subject only to the restrictions set forth below in the interest of public order.' With regard to possible attacks on religions and personal beliefs, the authors Barb Amandine and Lacorne Denis return In their book 'Les politiques du blasphème' (2018), to the fact that 'in France, a secular and pluralist society, respect for all religions goes hand in hand with the freedom to criticise religions of any kind and the freedom to represent subjects or objects of religious veneration. Blasphemy that offends divinity or religion is not repressed.'

To discuss a subject that relates to our cases, and illustrate, it may be interesting to look at the 'Extent of the lawyer's freedom of expression', from the title of the article posted on 'Le blog de Maître LBV'. In this regard, Article 41 of the Law on freedom of the press from 1881 is intended to guarantee what is called for convenience 'immunity of dress' and provides: 'No action shall be brought for defamation, insult or insult, neither the faithful account given in good faith of the judicial proceedings, nor speeches made or writings produced before the courts'. Obviously, this freedom is limited since 'Judges, seized of the case and ruling on the merits, may nevertheless order the suppression of injurious, insulting or defamatory speeches and condemn that it shall be subject to damages.' However, defamatory facts unrelated to the case may give rise either to public action or to civil action by the parties, when such actions have been reserved to them by the courts, and, in any case, to civil action by third parties. However, we can clearly see here the legislator's will to make this essential freedom prevail even within the walls of the judicial institution, a place where it would be unthinkable not to find it. The law of 15 June 1982 following the 'Choucq' case in 1980 also abolished the offences of audience.

With regard to the freedom of expression of lawyers outside the courtroom, although the debates are more topical than ever, the authors consider that, at the instigation of the European Court of Human Rights in particular, it should be considered that this reservation, as well as the professional secrecy of lawyers, could be specifically waived in the context of a public matter that has received media coverage. Obviously, most professions fortunately enjoy this freedom, but it is also clear that this concept, which is constantly evolving, often tends to be more and more widespread, particularly at the instigation of supranational institutions.

With respect to labour relations, we can consider how notions such as the right to expression arises from this cardinal notion of freedom of expression. The Article L2281-1 of the French Labour Code provides that 'employees have the right to direct and collective expression on the content, conditions and organisation of their work.' Subject to respecting his obligations of discretion and loyalty, the employee must be able to enjoy his freedom of expression.[578] This major principle prevails within and outside the company.

Another very interesting point at a time when more and more scandals are emerging, each time more relayed by information networks, Nicolas Malherbe stated that 'The dismissal of an employee who has reported in good faith to the public prosecutor facts likely to constitute criminal offences shall be null and void pursuant to Article 10 Section 1 of the European Convention on Human Rights (Conv. EDH).'[579] In addition to the Internet, which, governed by the Act of 21 June 2004, allows international communication in a very short space of time and is therefore an indispensable element in guaranteeing freedom of expression, 'Le monde politique' rightly points out that 'demonstrations and assemblies, as far as collective freedoms are concerned, are permitted and allow for the exercise of freedom of expression. Assemblies are not subject to any prior declaration and are relatively free. However, demonstrations regulated by the Decree-Law of 23 October 1935 are subject to prior declaration.'

To add a few more words on freedom of expression, which with regard to pamphlets, caricatures, pastiches or other forms of humour, freedom of expression allows the comedian to force features (thus inevitably questioning the admission of a certain right to excess), even if it means distorting reality. The judges do not hesitate to recognise 'a right to disrespect and insolence'.[580]

---

578 Cass. soc. 14-12-1999 n° 97-41.995 PB : RJS 2/00 n° 192 ; 22-6-2004 n° 02-42.446 F-P : RJS 11/04 n° 1120

579 Nicolas Malherbe, 'La liberté d'expression protectrice des salariés lanceurs d'alerte de bonne foi' (2016) LPA 6.

580 TGI Paris, 17th c., 9 January 1992: Gaz Pal 92-1, 182.

Brilliant or mediocre, the comedian must be able to express himself. The courts do not intend to set themselves up as contemptuous of bad taste, however proven. 'The humorist genre allows exaggerations, distortions and ironic representations, on the good taste of which everyone is free to judge'.[581] In the case of De Haes and Gijsels, it considers that the latter applies both to ideas which are 'favourably received' and to those which 'offend, shock or disturb.'[582] Inevitably, therefore, we see the extent to which French law may be influenced by European law, in particular.

In addition to the Constitutional Council and its jurisprudence, which states that 'This fundamental freedom [the free communication of thoughts and opinions] is all the more precious as its exercise is one of the guarantees of the right to freedom of expression. Essential for the respect of other rights and freedoms and national sovereignty', the European Convention on Human Rights, by which France is bound, provides that 'everyone has the right to freedom of expression', including freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers - Professor at the University of Rennes 1, Anne-Marie LE POURHIET reminds in this respect (L'encadrement juridique de la liberté d'expression en France) that in the H*andyside v. United Kingdom* judgment (7 December 1976) that the ECHR makes freedom of expression one of the essential foundations of a democratic society and one of the essential conditions for its progress and the fulfilment of each individual. The scope of freedom of information is, in particular as a result of European Law, tending to widen as it now includes the press, television, internet, works of art, etc. In recent years it has probably been noted that the Court has had an increasingly broad notion of the concept of general interest. In the first *Von Hannover v. Germany*, judgment of 24 June 2004, the Court held that elements relating to the private life of Princess Caroline of Monaco did not fall within the general interest. However, in a judgment of 19 September 2013, *Von Hanover v. Germany No. 3*, the Court considered that photographs showing the Princess on holiday with her husband contributed to a debate in the public interest because they illustrated, *inter alia*, a tendency for famous people to rent out their second homes. Freedom of information also presupposes the protection of sources of information. An obligation to disclose sources can only be reconciled with Article 10 if it is justified by an overriding requirement of public interest.[583]

581 Paris Court of Appeal, 11 March 1991, 18 February 1992' 95 Légipresse 112.
582 *De Haes and Gijsels v. Belgium* App no 19983/92 (ECtHR 24 February 1997)
583 *Becker v. Norway* App no 21272/12 (ECtHR 5 October 2017)

The lawyer's freedom of expression outside the courtroom, as mentioned above, is less extensive than that of the journalist, inasmuch as the European Court considers that the exercise of this freedom must remain compatible with the contribution which the lawyer must make to the trust in the public service of justice. However, there has been a trend towards greater freedom of expression for lawyers, notably in a Grand Chamber decision, CEDH, gr. ch. *Morice v. France* 23 April 2015. The Court considers that the conviction of a lawyer for defamation on account of remarks made in the press against an investigating judge violates Article 10 of the European Convention of Human Rights by reason of the penalty imposed, since his remarks raise a debate in the public interest and are based on a sufficient factual basis.

To conclude, we therefore see a protection of freedom of expression by France, both at the level of its constitutionality block, of the case law that has been built up over time, and from the point of view of France's supranational commitments, whether from the point of view of the European Convention on Human Rights (ratified by France in 1974), the International Covenant on Civil and Political Rights (16 December 1966) (in line with the rights defended by the Universal Declaration of Human Rights).

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

The French government has decided to apply the law relating to the state of emergency - necessary to prevent the perpetration of new terrorist attacks. Certain measures are likely to involve derogation from the obligations arising from the Convention for the Protection of Human Rights and Fundamental Freedoms. The government thus notified the Council of Europe in 2015 that the state of emergency would lead to derogations and restrictions considered necessary for certain human rights.

The *procédure de notification de contenu illicite sur internet* (which can be translated as 'procedure for notifying illegal content on the Internet' is a provision of the French law on confidence in the digital economy of 21 June 2004 known as the LCEN law. The aim is to obtain the removal of any illegal content appearing on a website or the blocking of the site by the host, before any intervention by the judicial authority.

Article 4 of the Loppsi 2 LAW No. 2011-267 of 14 March 2011 (Law of Orientation and Programming for the Performance of Internal Security), which establishes a blocking system for sites that disseminate child pornography

content, is for its part declared 'in conformity with the Constitution.' The decision No. 2011-625 DC of 10 March 2011 of the Constitutional Council states that 'Considering that Article 4 of the referred law inserts two paragraphs after the fourth paragraph of Article 6 of the aforementioned law of 21 June 2004, according to which : 'Where justified by the need to combat the dissemination of images or representations of minors covered by Article 227-23 of the Criminal Code, the administrative authority shall notify the persons mentioned in paragraph 1 of this I of the electronic addresses of online public communication services that contravene the provisions of this Article, to which these persons must prevent access without delay.'

'A decree in Council of State shall lay down the procedures for applying the preceding paragraph, in particular those according to which the additional costs resulting from the obligations imposed on operators shall be compensated, where appropriate.' On the other hand, the collective la Quadrature du Net notes that 'A draft European regulation uses the pretext of the fight against terrorism to impose heavy obligations on all hosts, including the withdrawal in one hour of content reported by the police.' Regarding to recent legislation, the law of 22 December 2018 on the manipulation of information creates a new injunction, during the three months preceding an election, to stop the dissemination of 'inaccurate or misleading allegations or accusations of a fact likely to alter the sincerity of the forthcoming elections [...] disseminated in a deliberate, artificial or automated and massive manner through an online communication service to the public.' Still concerning the risks linked to terrorism, Article 6-1, created by law n°2014-1353 of 13 November 2014 - Article 12 indicates that 'When justified by the needs of the fight against provocation to terrorist acts or the apology of such acts falling under Article 421-2-5 of the Criminal Code or against the dissemination of images or representations of minors falling under Article 227-23 of the same Code, the administrative authority may ask any person mentioned in III of Article 6 of this Act or the persons mentioned in 2 of I of the same Article 6 to withdraw content that contravenes these same Articles 421-2-5 and 227-23. In the absence of withdrawal of such content within a period of twenty-four hours, the administrative authority may notify the persons mentioned in the same one of the lists of electronic addresses of online communication services to the public that contravene the said Articles 421-2-5 and 227-23. These persons must then immediately prevent access to these addresses.'

In any case, moderation of his remarks on the Internet and the prohibition of defamatory remarks are cardinal principles since 'Public insult, i.e., disseminated on a network or site accessible to all, is an offence punishable by a fine of €12,000. If the insult is discriminatory (racist, homophobic, against disabled

people...), you will incur a 6-month prison sentence and risk paying a €2,500 fine. Private insult, i.e. accessible to a limited number of people, is a fine of €38; €750, if the insult is discriminatory (racist, homophobic, against the disable). If the comments are broadcast on an account accessible to all, the defamation is public and constitutes an offence punishable by a fine of €12,000.' And 'If the profile is only accessible to a limited number of people, it will be a private defamation, a fine of €38.'

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

On 15 February 2016, the Council of State rejected two appeals against the procedure that allows the Ministry of the Interior to order the blocking and dereferencing of websites without their illegality being confirmed by a judge. Less than a week after ruling that access to Internet users' connection data by the intelligence services was not disproportionate, the Council of State on Monday rejected two appeals against the blocking and dereferencing of websites imposed by order of the Interior ministry.

The French Data Network (FDN), the Fédération FDN (FFDN) and La Quadrature du Net (La Quadrature du Net), which challenged the legality of two decrees published at the beginning of 2014, in application of the anti-terrorism law of 13 November 2014 and the Loppsi law of 14 March 2011: Decree No. 2015-125 of 5 February 2015 relating to the blocking of sites provoking acts of terrorism or apology and sites broadcasting images and representations of minors of a pornographic nature; Decree no. 2015-253 of 4 March 2015 relating to the dereferencing of sites causing acts of terrorism or in apology and sites broadcasting images and representations of minors of a pornographic nature.

Recent statements by French President Emmanuel Macron in a speech to UNESCO on the occasion of the 30th anniversary of the International Convention on the Rights of the Child remind us that in France measures to protect vulnerable people can lead to restricting the access of certain groups to the Internet. On this subject, Emmanuel Macron gave 'six months to digital platforms and operators to propose "robust solutions" aimed at protecting children in the digital space, failing which the government will present a law-making parental control on the Internet automatic.'[584]

[584] Marine Pennetier, 'Macron menace d'une loi sur un contrôle parental automatique' (*Thomas Reuters À la une,* 20 November 2019) <https://fr.reuters.com/article/topNews/idFRKBN1XU17K)>.

While the Government may initiate such filtering, restrictions may apply in the context of corporate access for business use, to protect individual liberties, or for educational use. Generally, private use of computers and the Internet is tolerated by the employer. However, according to the CNIL (*Commission nationale de l'informatique et des libertés*), this use must remain reasonable, and must not threaten the security of the company's network or slow down its productivity.[585]

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a branch of the Central Directorate of the Judicial Police, aims to prevent the publication of content of a pornographic nature, inciting or advocating terrorist acts. In 2016, the CNIL examined no fewer than 5,512 requests related to these decisions.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In France, if freedom of expression is one of the most important freedoms it should never overstep interests protected under Article 10(2) of the European Convention of Human Rights (ECHR).[586] As there is an independent organisation in charge of controlling Medias such as television or radio it would be logical to have such an organisation for online content. [587] However, in France there is no such organisation for online content and self-regulation is the rule for ensuring the protection of freedom of expression online.

It is true that the CSA as many times shown an interest on taking control on this matter but without any success self-regulation remains the rule.[588] Nevertheless, courts of justice can influence those self-regulation systems by forcing them to intervene by blocking and taking done some specific contents. For example, in 2013 a French court of justice[589] ruled that Twitter France has to identify authors of anti-Semitic messages 'within the framework of its French site'.[590] While

585 'Internet au travail: ce qu'il faut savoir' *Journal Du Net* (18 January 2019) <https://www.journaldunet.fr/management/guide-du-management/1201587-internet-au-travail-ce-qu-il- faut-savoir/>

586 The Swiss Institute of Comparative Law, 'Comparative study on blocking, filtering and take-down of illegal internet content' (Council of Europe, 2015) <https://www.coe.int/en/web/freedom-expression>

587 CSA, Conseil Supérieur de l'Audiovisuel < https://www.csa.fr>

588 Jean-François Sacré, 'Le CSA veut réguler les réseaux sociaux' *L'Echo* (5 February 2020) <https://www.lecho.be/entreprises/media-marketing/le-csa-veut-reguler-les-reseaux-sociaux/10205928.html> accessed 1 March 2020

589 UEJF, 'TGI de Paris' *(Twitter,* 24 January 2013).

590 Wolfgang Benedek and Matthias Kettemann, *Freedom of expression and the internet* (Council of Europe Publishing 2013)

private sector companies of online content apply self-regulation the French legislation and its judicial system can always keep an eye on this self-regulation. Associations or individuals can ask the court to force self-regulated companies to block or to take down some content in the name of the protection of freedom of expression. Those safeguards are not totally efficient but are a first step in the road for a better control of freedom of expression and self-regulation of content online.

Few safeguards have been enforced so that private sectors can keep ensuring the protection of freedom of expression online while applying self-regulation for public order. Some information is given beforehand to the user, to make sure that he knows what would be unacceptable and would, therefore, give rise to a block of content. However, French law does not seem to give many prerogatives to users after private sectors take down or block illicit contents. This has been the most criticised point, and what is considered lacking in French law in regard to the issue of blocking and taking down of internet content.[591]

An ongoing project has been established to reinforce the mechanisms that have been created. Particularly by creating a duty of care of the private sectors towards the users that have been victims of illicit contents. The goal is also to reinforce what happens upstream. The key word that French law is considering is transparency.

Transparency towards the users; they now need to be aware of the conditions in which they are allowed to express themselves, the limits to their freedom. French law wants to make sure that the safeguards and mechanisms created are all accessible to all citizens, sort of a reasonable man test. In fact, if the algorithms are not understood by the users, they could be misused and diverted from their main and initial goal. Transparency can take different forms. For instance, a regular citizen without any technical knowledge whatsoever, can communicate the criteria that determined a certain result in regard to these actions. In this case, the transparency is not only beforehand but also after the facts. It could also be justifying the decision of taking down a post, or an absence of response after reporting content.

Transparency will force the private sectors to justify their decision and therefore legitimise it in a way, and also give feedback to the user by explaining what went wrong.

591 Rapport of the working group 'Régulation des réseaux sociaux – Expérimentation Facebook » sent to State Secretary in Charge of digitalisation, May 2019.

However, it has been agreed that transparency can not only be declarative, a system must be conceived to verify the algorithms used by private companies. Mechanisms of compliance need to be created for a better application of transparency.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

The right to be forgotten consists in two rights: The right to Erasure and the right to dereferencing. The first one is based on a legal text, the French Data Protection Act from the 6 January 1978, and also, at a European level, on the General Data Protection Regulation (27 April 2016). The second one was created by the European Court of Justice, in the decision *Google v. Spain*, 13 May 2014.

The right to erasure is based on both the Article 51 of the French Data Protection Act, and the Article 17 of the General Data Protection Regulation. It consists in the right for an individual to obtain from the controller of the data the erasure of personal data concerning him or her without undue delay.

The request must be directed to the controller of the data, that is the editor of the site on which the personal data are displayed. The controller of the data has a deadline of one month starting from the day he received the request to erase the personal data, or answered the request. In case of non-performance of the obligation to erase personal data in due delay, the data subject can refer the matter to the National Commission for Data Protection (CNIL). The National Commission for Data Protection has a deadline of three weeks to give a decision.

Pursuant to Article 51 of the French Data Protection Act, when the controller of the data has transmitted it to a third party, he has to take all reasonable measures in order to inform the third party that the data subject has requested the erasure of their personal data.

The right to erasure is not an absolute right. There are a huge number of situations in which this right to erasure does not apply. It is the case when applying it would go against the exercise of freedom of speech and the right of the public to be informed. It is also the case when the data controller is under a legal obligation, whether coming from French or European law, to save and keep the data, or when the data controller carries out a mission of public interest. The right to erasure is also limited by the need to save and preserve data for archival purposes, for historical or scientific research purposes, and for the establishment, exercise or defence of legal claims.

The right to dereferencing was created by the European Court of Justice in its famous decision *Google v. Spain* from 13 May 2014. It hasn't been included in the General Data Protection Regulation. In this ruling, the European Court of Justice decided that internet users could request search engines to delete the links associated with their name and surname which are giving access to web pages affecting their privacy. The right to dereferencing derive from the right to be forgotten.

Search engines' mission consists in indexing data and classifying it in order to present it to internet users in a given order of preference. Therefore, they are likely, when a search associated with an individual's name and surname is made, to display links giving access to personal data about the individual. That is the reason why the European Court of Justice considers that the right to dereferencing is a necessary complement to the right to erasure, in order to ensure an efficient protection of personal data.

The Court of Justice of the European Union considers that the right to dereferencing must not only prevail on the economic interest of the search engine operator, but also, on the public's interest to have access to the information when doing a search associated with an individual's name and surname.

Concerning the territorial scope of the right to dereferencing, the Internet has been a global network with no borders, search engines enable the permanent access to information displayed after a search. That is why, the matter of the geographical extent of the right to dereferencing is crucial.

In a decision given on the 24 September 2019, the European Court of Justice delineated the geographical scope of the right to dereferencing. The dispute concerned the French National Commission for Data Protection (CNIL) and a search engine operator, Google Inc.

The French National Commission for Data Protection (CNIL) had required Google Inc. To perform the dereferencing requested on each extension of the domain name of its search engine, and not only on the national domain name of the applicant. The search engine operator refused alleging that it would put at risk freedom of expression. The European Court of Justice declared that the European regulation does not impose a global dereferencing, i.e., on every extension of the domain name of the search engine. However, the dereferencing must be executed on every extension corresponding to a European domain name, and not only on the extension corresponding to the national domain name.

Moreover, the search engine operator must ensure the efficiency of personal data protection by taking all appropriate measures to prevent or seriously deter internet users from accessing the litigious links. In practice, it involves the implementation of a geo-blocking device, which allows preventing the possibility of accessing the litigious links, from an IP address known as located on the territory of a Member State, irrespective of the extension of the search engine that is used.

The right to dereferencing is not absolute. The Court of Justice of European Union said so in a decision from the 24 September 2019. Preliminary questions had been referred to the European Union court of justice by the French Administrative Supreme Court, the Council of State. The Court of Justice of the European Union declared in this decision that the right to dereferencing must be put into balance with fundamental rights such as freedom of expression and the public's right to be informed. The balancing of interests must be done according to the principle of proportionality. It has to be determined whether or not the litigious webpage is necessary for the information of the public.

After the Court of Justice of the European Union declared that the right to dereferencing was not absolute, the French Council of State issued 13 decisions on 6 December 2019, defining the limits of the right to dereferencing.

They distinguish between three types of data and define the appropriate extent of protection for each of these three categories of data. The three categories are the following: criminal data which are related to legal proceedings or criminal convictions, personal data that are sensitive and personal data that aren't sensitive. Sensitive and criminal data benefits from a particularly high protection. The French Council of State, in its decisions issued on 6 December 2019, stated that a dereferencing request regarding sensitive criminal data can only be refused if their access is strictly necessary for the information of the public.

Regarding non-sensitive personal data, their protection is weaker. A dereferencing request concerning non sensitive data can be refused as long as an overriding interest of the public to have access to the data exists.

To determine whether or not a dereferencing request must be completed, the balance has to be made between two fundamental rights: the public's right to be informed and the right to privacy of the data subject.

Sensitive data are the ones that are more intrusive into the private life of the data subject. The French Council of State considered as sensitive data the sexual orientation of a plaintiff who requested the dereferencing of links giving access

to a literary website that, while relating the content of an autobiographical novel written by the plaintiff himself, revealed his homosexuality.

The Council of State also considered as a sensitive data the religious affiliation, in a case regarding a press article mentioning the former affiliation of the plaintiff to the Church of Scientology.

Sex life and especially extramarital relationships are also considered as sensitive data. The Council of State declared justified the dereferencing of a video revealing an extramarital relationship of the applicant and a statesman, considering that this information does not contribute to any debate of general interest.

The address is also considered a sensitive data. The Council of State considered the dereferencing request of an applicant who registered a patent, given that the web pages regarding his patent mentioned his address.

However, the Council of State did not consider the request of a doctor aiming at dereferencing links giving access to a website providing his professional address and enabling the internet users to make comments. The Council of State declared that there is an overriding interest for the public to access that information when making a search associated with the doctor's surname.

The Council of State outlined the criteria which are to take into consideration to appreciate the strictly necessary character of an information or the existence of an overriding interest for the public to have access to it.

One of those criteria is the nature of the data. The Council of State decided that when the data concerned consist in several press articles mentioning a criminal conviction of glorification of war crimes or crimes against humanity, the public information is strictly necessary and must prevail over the protection of personal data.

Another of those criteria is related to the accuracy and the source of the data. The Council of State asserted that even when the data are coming from a lawful press article and the data are accurate, privacy protection considerations can justify the dereferencing. Regarding the case of the press article mentioning the former affiliation of the applicant to the Church of Scientology, the Council of State considered that the accuracy of the information does not justify maintaining the access to the data involved, especially given that the applicant did not have any link with the organisation anymore for more than 10 years.[592]

[592] Decision of the State Council, 6 December 2019 nº 393769

The impact that the referencing of the data is likely to have on the data subject's life is another of the criteria to take into consideration. Regarding a children's leader who had been convicted to seven years of prison sentence for sexual assault on minors and is still under legal supervision, the Council of State decided that the dereferencing was justified considering the impact that maintaining those data accessible when making a search associated with the applicant's name would have on the data subject's reintegration.

Similarly, regarding the press article mentioning the former affiliation of the applicant to the Church of Scientology, the Council of State decided that the dereferencing was justified especially in view of the serious impact maintaining those data indexed would have on the applicant's life.

The notoriety of the individual involved is also an element to take into consideration. The Council of State rejected a request for dereferencing of links giving access to interviews in which an actress discussed her criminal conviction for domestic violence. The Council of State considered that given the actress's notoriety, the indexing of the litigious links was strictly necessary to the information of the public.

In the case with regard to a criminal conviction for sexual assault on minors, the Council of State pointed out that the applicant had no notoriety; therefore, the referencing of the litigious links was not strictly necessary to the information of the public.

The function of the data subject in the society and its eventual role in the public life also has to be taken into consideration. The Council of State decided that maintaining the referencing of links giving access to press articles reporting the criminal conviction of an actual mayor and former deputy for glorification of war crimes and crimes against humanity is strictly necessary to the information of the public, even though the Court of cassation quashed the conviction. The Council of State decided so especially in view of the data subject's role in the public life.

The possibility to have access to the same information searching from key works that do not include the name of the individual involved is also one of the criteria to take into account.

The role played by the data subject in the revealing of the information has an impact on the decision to maintain or not the referencing of the litigious links. The Council of State considered justified the dereferencing request regarding links giving access to a literary website revealing the homosexuality of an autobiographical novel's author even though the information had been revealed

by the author himself in the first place. The Council of State indicated that the novel was no longer edited, and the applicant did not have literary activity anymore.

However, regarding the actress who discussed her criminal conviction for domestic violence in interviews, the Council of State refused the dereferencing request considering that she decided voluntarily and freely to speak about it.

Regarding criminal data, the Council of State considered that when examining cases in which the indictment led to discharge or acquittal of the indicted person, the requests aiming at the dereferencing of press articles dealing with the indictment of the person had to be granted.

This does not apply when the seriousness of the facts and the notoriety of the person are such that the referencing of the litigious data is strictly necessary for the information of the public. The Council of State ruled in this way regarding the case of press articles dealing with the criminal conviction of a mayor and former deputy for glorification of war crimes and crimes against humanity, even though the conviction had been quashed by the Court of cassation. The Council of State specified that the litigious press articles referred to the actual and accurate judicial situation of the person in question, as they mentioned the decision of the Court of cassation.

In another case about criminal data,[593] the Council of State emphasised that when the litigious link give access to a webpage dealing with a step of the judicial proceeding which does not correspond anymore with the actual judicial situation of the person concerned, but keeping this data referenced is considered strictly necessary to the information of the public, the search engine's operator must arrange the list of search result. It has to be presented in a way that before the litigious links appear; at least one link giving access to a webpage referring to the accurate and actual judicial situation of the person had to pop up.

The Court of cassation referred explicitly to the European Union Court of Justice decision of 24 September 2019, in a decision issued on 27 November 2019. The case was about a dereferencing request from an expert accountant concerning a press article dealing with his conviction for fraud. The Court of cassation quashed the decision of the Court of appeal of Metz affirming that the indexing of the litigious links in the search result list, when the search is associated with the person's surname, was strictly necessary for the information of the public.

593 Conseil d'Etat, 6 December 2019 n° 401258.

6. How does your country regulate the liability of internet intermediaries?

At the national level, electronic commerce is regulated by the law '*Law on confidence in digital economy*' from the 21 June 2004, which is the law implementing the European directive.

Two types of internet intermediaries have to be distinguished: internet access provider and hosting provider. There are two different regimes under the aforesaid law: the non-liability of internet access providers and the limited liability of hosting providers.

The internet access providers are defined by the law as 'people whose activity is to provide access to online public communication services.' They provide a service consisting in the transmission of data and in this way, they enable their clients to access the Internet. The main internet access providers in France are Orange, Free, Bouygues Télécom and Numericable-SFR.

The national law as well as the European directive establishes the principle of non-liability of the internet access provider. Article 9.I of the '*Law on confidence in digital economy*' excludes both civil and criminal liability of the internet access provider. This Article sets up three derogations that are three cases in which the liability of the internet access provider could be incurred. The common link between those three cases is that the internet access provider goes out of its strict mission of data transmission. In fact, in those three cases the internet access provider does not limit its action to the sole transmission of data; it interferes with it whether by initiating the transmission of data, or by selecting the recipient of it or by modifying the information that is being transmitted.

An internet access provider can only see its liability be incurred if it goes out of its sole and strict data transmission role. This mission must be performed in a neutral way without interfering in the transmission, in order to ensure the non-liability of the internet access provider.

Besides, the '*Law on confidence in digital economy*' does not impose any general monitoring or control obligation to the internet access provider over the data they transmit. There is also no general obligation to look for facts or circumstances revealing illicit activities. Article 6 of this law excludes every control obligation, inquiry obligation and even filtering obligation regarding the data transmitted by the internet access providers and the data flowing on the Internet.

Nevertheless, internet access providers have an obligation to put into effect every request coming from a judicial authority asking them to carry out 'a targeted and temporary surveillance.'

The hosting providers are defined as those who are in charge of 'the storage of signals, writings, images, sounds or messages of any kind provided by recipients of online public communication services.' In practice, they provide a storage service for their clients' web pages and websites.

Their liability is restricted. It can only be incurred if the hosting provider was aware of the unlawfulness of the content stored and did not proceed to the prompt and complete withdrawal of it. This rule applies to both civil and criminal liability according to Articles 6.I.2º and 6.I.3.

In a similar way as for the internet access provider, the law *Law on confidence in digital economy* does not impose any general surveillance or control obligation to the hosting provider over the data they store. In the absence of a general obligation of supervision, the hosting provider is not expected to look for illicit content within the data they store. They are therefore not aware of the content they store and cannot be expected to be aware of the potential unlawfulness of some of this data. They elude liability by their non-knowledge of the data they store and non-awareness of their illicit nature. Nevertheless, a third person can draw their attention to the illicit nature of some of the content they store. In this hypothesis, in order to elude liability, the hosting providers must proceed to the prompt withdrawal of the illicit data.

There is a notification procedure enabling internet users to report to hosting providers the existence of illicit content. According to Article 6.I.5º of the *Loi pour la confiance dans l'économie numérique*, the notification allows to presume that the hosting provider was aware of the illicit data stored. To create a presumption of awareness, the notification must contain a certain amount of elements such as the date of the notification, the identity of the person who notifies, the description of the litigious facts and the exact web pages concerned, the motives and the legal ground justifying that the content must be withdrawn. Besides, before the notification proceeding the notifier must beforehand have informed the editors of the concerned webpages asking for their withdrawal or modification. The notification must contain a copy of the request addressed to the editors or evidence that the editors could not be contacted.

The Court of Cassation affirmed the mandatory nature of every element of the notification. The notification in order to have probative value must be complete, which means that it must contain each of the elements described in the Article 6.I.5º of the law to support confidence in the digital economy.

Same law imposes that the Internet access providers and hosting providers are not under a general surveillance obligation over the data they transmit or store, however they must collaborate with public authorities to fight against illicit activities. They have a double obligation to promptly inform the public authorities of every illicit activity that has been reported to them and to take all the appropriate measures to fight against those illicit activities and to make public the means they devote to it. Those obligations aiming at the collaboration of internet intermediaries are described in the Article 6.I.7º of the *Law on confidence in digital economy*.

Among the measures to fight against those illicit activities is the obligation to set up an easily accessible mechanism enabling every internet user to draw the attention of internet access providers and hosting providers to the existence of illicit information or activities.

Among those measures, there is also the blocking of access to illicit content. The Court of Justice of the European Union declared, in two decisions of 2012 and 2011, to be opposed to a general filtering obligation. Nevertheless, it does not prevent the possibility to take moderated blocking measures.

Article 6.I.8º of the law *Law on confidence in digital economy* states that a judiciary authority can prescribe to every internet access provider and hosting provider in an emergency interim proceeding 'to take every appropriate measures in order to prevent a damage or to aim at the cessation of a damage caused by the content of an online public communication service'. This provision creates a new emergency interim proceeding, called the Internet interim proceeding. The particularity of it is that it is directed to Internet access providers and hosting providers, in order to make them collaborate with the public authorities to fight against illicit content.

The blocking of illicit content can also be requested by an administrative authority. It is possible in case of content related to terrorism and child sexual abuse images. This possibility is stated by the Article 6-1 of the law. The mechanism of the blocking request made by an administrative authority is deployed in two steps. First, the administrative authority must request the website editor and its hosting provider to withdraw the illicit content. Then, in the absence of withdrawal of the illicit content in a delay of 24 hours, the administrative authority can notify the litigious content to the internet access provider 'which has to prevent without delay the access to those online addresses.'

The existence of the administrative blocking mechanism can be questionable in terms of guarantee of individual liberties given that no judge intervenes in this mechanism.

Article 6-1 of the law provides for a control of the administrative blocking measure by a qualified personality designated within the administrative authority itself by the National Commission for Data Protection (CNIL), whose mission is to ensure the protection of privacy and individual liberties.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

The right to be forgotten has been discussed a lot in legal circles; there have been many misunderstandings about its application. It requires the organisation to erase the personal data of a person within one month if: personal data is no longer necessary for the initial purpose, the data subject withdraws consent, the data subject objects to the processing or if data is unlawfully processed.

If one or more of these grounds apply, reasonable steps to erase the personal data must have been taken. This includes requesting third parties to remove such data as well. If one organisation has made the personal data public, it should also inform other parties who process the personal data. However, the right to be forgotten is not absolute. A request for deletion can be denied, for instance, in cases where freedom of expression and information must prevail. As GDPR introduces a right for individuals to have personal data erased, the right to erasure is also known as the right to be forgotten. Individuals can make a request for erasure verbally or in writing. The right is not absolute and only applies in certain circumstances.

This marks an important milestone in the adoption of the General Data Protection Regulation and of the Data Protection Directive as four years have passed since their official first draft release, on 25 January 2012, which promised greater EU personal data protection and a modern and harmonised data protection framework across the European Union.

The Directorate for Personal Data Protection (DPDP) points out that if the current regulation is considered to be some kind of basic level of personal data protection, the new regulation will mean a higher level of protection. It enables the citizen or entity to have greater control over their personal data because now

the data processing, in addition to what should be fair and in accordance with the law, should be transparent. Transparent processing means that every subject of personal information has to be informed of the purpose of the collection, processing and storage of their data. They must also be informed of the identity of the controller of their data, and the users of their data. The period of storage must also be reported, and the subject has to be provided with access to their data at any time, this will ensure greater control of their data. If any incident occurs, the controller is obliged to notify the entity that its data has been compromised.

This regulation implements two new rights: The right to be forgotten and the right to have its data transmitted to another controller.

The right to be forgotten implies that the subject may at any time request that their personal data be deleted from the Internet or his history. This right to be forgotten first arose from the requirement of citizens to restrict the further processing of their personal data online, and to prevent permanent or periodic stigmatisation as a result of their conduct and past activities. If the data is not deleted, the data subject will have the right to go to the body for protection of personal data. Each auditor will need to determine the purpose of storing personal data and the time it will take to accomplish that goal.

With respect to data transmission, the entity may require the controller to provide it in a readable form so that it may transmit it to another controller. This means that as long as the citizen has provided their information such as email, address, mobile number and has accepted to be sent a text message for direct marketing or advertising needs, he may request the company to erase them. However, data transmission has more to do with another type of data processing, namely, what is known as big data, involving companies like banks, social networks, telecommunications operators or online sales platforms. These companies or controllers will be required to provide such technology that can transmit data in machine-readable form. If the citizen asks for his data to be given on CD, then the company would have to hand it over so that the data can read and transmit for him, to be understandable. In the US, companies now have different software solutions, but then those solutions i.e., applications have to be compact.

In conclusion, it is difficult to imagine the development of this right in France within the five upcoming years, considering the potential changes in the EU legislation, domestic and European anti-corruption policies and gender equality.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

As Internet's most popular social networks enter their tenth, fourteenth and even sixteenth year of service, their users are growing more and more concerned about their fundamental rights. It seems that since a couple of years now, people are not as careless with their personal data as they used to be. Part of that thanks to media outlets that highlighted wrongful practices from the most popular social networks. As the social climate heats up in the whole world, the Internet has become a double-edged sword: knowledge is available to all, but anyone can proclaim himself an expert which eventually leads to false information.

France's overuse of legislation as an answer to any sort of problem has not yet reached the topic of Internet censorship, freedom of expression online or protecting hate speech. This ambiguous situation only tells how big of a problem this has become, as the tools once imagined by the political class are now outdated.

Nevertheless, France's legislation lies on ancient foundations like the Declaration of the Rights of the Man and of the Citizen of 1789 and especially Article 11, stating 'the free communication of ideas and opinions is one of the most precious rights of man'. Two hundred and thirty one years later, this basis is still very well applied and in effect but as we proceed to analyse the situation of Internet censorship in France, this Article as well as the whole Declaration underlines very well the current issue of reaching a balance between freedom of expression and protecting hate speech in the online environment.

Therefore, France's legislation of the issue relies mostly on a legal basis that still has an impact today, but some see the need for a change and the urgency to address the matter. Hence, there is a necessity for the evolution of the French legal framework. It can be considered that the French government made certain steps forward with the adoption of the '*Loi on confidence in digital economy*' and another law – '*Loi on digital Republic*' issued on 7 October 2016.

The question that might be asked is – which legislative measures are taken in 2020, when we are entering a new digital age and the new digital rights need to be assured. It is certain that France is in the process of making a long-lasting change in the legal landscape, especially with the 'project-law' AVIA. Although France is moving forward, this law has been the object of numerous critics, such

as one by B. Retailleau regarding the fear of censorship. Additionally, he compared French and German systems.

Moreover, in one report published by Institute for Strategic Dialogue, an independent organisation, additional critiques were addressed. They concluded that there are limits concerning certain algorithms about censorship of hate language on the Internet. Research shows that more than 85% of the hate speech content has been removed, which raised concerns in this Research Group. In the above-mentioned report it is stated that artificial intelligence cannot replace human work and human emotions regarding hate speech on the Internet – which shows that there are some 'gray zones' of the permitted content, when it comes to hate speech on the internet.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

Although one of the most prestigious reports in the sphere of the Internet censorship 'Freedom on the Net', Freedom House Annual Report, classified France as a country with Internet freedom, there are some serious restrictions existing.

The State Council and Constitutional Council are exercising something known as 'control of the proportionality' between European and domestic legislation, as well as if the measures taken regarding the censored content are necessary, adequate and proportionate. Following this frequently used rule in French legal system, President Macron declared his worry and willingness to establish a more severe legislation against racism on social media and stricter control over hate speech on the internet.

As France is classified as one of the top 12 countries regarding the Freedom of expression on the internet, it can be considered that balance is very well achieved, but it is not always the case in practice, according to the previously mentioned report of Freedom House. With the application of the 'proportionality rule', national judges have a large merge of the appreciation and huge liberty when it comes to decision making if the concrete content should be removed or not.

10. How do you rank the access to freedom of expression online in your country?

Last year, the French President Emmanuel Macron declared his willingness to establish a tougher legislation against racism on social media channels with the removal of hateful comments online, the identification of the perpetrators and their banishment on websites.

It is important to underline that in France, there is no specific law on the freedom of expression online but there is a growing desire to establish a legislation which follows the advanced German model.

Moreover, the 'Loppsi Law' voted in March 2011, authorised the administration to block websites with potentially objectionable content. A secret list has been drawn up with the several websites which are likely to be blocked by the French administration.

This law has been strongly criticised due to its secret use and limits. That is why Benjamin Bayart, fundamental freedoms campaigner, qualified it as a 'secret police censorship.'

Even if there is no specific law on the freedom of expression online in France, some restrictions have been gradually established on special subjects (child pornography, racism, terrorism). Moreover, the internet hosts are now liable for the internet user's activities, as mentioned in the Yanick D. case.

Otherwise, the Constitutional Council declared that some restrictions can be authorised following strict conditions:[594] a general suspension of internet access can be set up which is clearly an infringement on the freedom of expression online.

The increase of these restrictive measures is explained by the state of emergency in France and the difficult and delicate balance between the freedom of expression online and the national security.[595] The Government can now block websites without the prior consent of the judge. With this decision, France might be punished by the European Court of Human Rights because of the violation of Articles 8 and 10.

Furthermore, it is difficult to rank the access to freedom of expression online in France. Some restrictions are explained by political reasons and others can be useful and necessary for national security.

---

594 Conseil Constitutionnel n°2009-580 DC du 10 juin 2009.

595 State Council decision from the 15 February 2016.

It is evident that in France our freedom of expression is practically uncensored but generally people censor themselves to the extent that most know what can and cannot be said. For those who do not differentiate between words such as homophobic, racist or cyber-harassment and freedom of expression, France is not as restrictive regarding freedom of expression as other countries. It is clear that there is a limit to freedom of expression, but it is not yet explicit.

11. How do you overall assess the legal situation in your country regarding internet censorship?

Following the analyses in the previous questions, it can be considered that there is medium internet censorship in France, but it is more legislated especially regarding child pornography, terrorism and racial hate. Additionally, intellectual property rights are well protected in French internet space because of the continuous attempts to protect copyright.

In the report by Freedom House known as 'Freedom on the Net' from 2015, France has been classified as a country with Internet freedom. Although considered as a 'free country', there still have been some journalists and bloggers that have been arrested because of the content they wrote.

Furthermore, there have been some changes in 2015, aftermath of the Charlie Hebdo terrorist attack, such as restrictions on content that could be interpreted as 'apology for terrorism', which can lead to significantly increased surveillance of the person.

The French government has taken various measures to protect the rights of the users on the internet, such as the entrance into force of the *Loi pour la Confiance dans l'Economie Numérique* (LCEN, Law for Trust in the Digital Economy) in 2004. This law was seen as a revolutionary one at the time. However, the passage of the new law regarding copyright threatens to ban users after their third violations – because of the rule known as 'three strikes rule' – which has drawn much criticism from privacy advocates as well as European Union Parliament. As a result of the application of the above-mentioned 'three strike rule', France has been added to the list of 'Countries Under surveillance' by Reporters Without Borders.

Conclusion

To conclude, it is hard to answer if France is a country with limitless freedom on the internet or a much censured one. Certainly, domestic legislators created numerous laws in order to regulate internet space in France, but those laws have not limited users' internet experience. Freedom House report mentioned in the analyses ranks France amongst the top 12 countries for Internet Freedom, which can be seen as a very good result and we can consider France as a country on the list of countries that are cautious, but not limitative towards its users.

Table of legislation

Provision in French language	**Corresponding translation in English**
Loi du 9 décembre 1905 concernant la séparation des Eglises et de l'Etat. - Article 1 : La République assure la liberté de conscience. Elle garantit le libre exercice des cultes sous les seules restrictions édictées ci-après dans l'intérêt de l'ordre public.	1905 French law on the Separation of the Churches and the State – Article 1: The Republic ensures freedom of conscience. It guarantees the free exercise of religion under the provisos enacted hereafter in the interest of public order.
LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure – Article 4 I. — L'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est ainsi modifié : 1° Après le quatrième alinéa du 7 du I, sont insérés deux alinéas ainsi rédigés : 'Lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai. 'Un décret fixe les modalités d'application de l'alinéa précédent, notamment celles selon lesquelles sont compensés, s'il y a lieu, les surcoûts résultant des obligations mises à la charge des opérateurs. ' ; 2° Au dernier alinéa du même 7 et au premier alinéa du 1 du VI, les mots : 'et cinquième ' sont remplacés par les mots : ', cinquième et septième '. II. — Le I entre en vigueur six mois à compter de la publication du décret prévu au sixième alinéa du 7 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et, au plus tard, à l'expiration d'un délai d'un an à compter de la publication de la présente loi.	Law n ° 2011-267, 14 March 2011 on orientation and programming for the performance of internal security - Article 4: I. - Article 6 of the law n ° 2004-575 of 21 June 2004 for confidence in the digital economy is thus modified: 1 ° After the fourth paragraph of 7 of I, two paragraphs are inserted as follows: 'When the needs of the fight against the dissemination of images or representations of minors under article 227-23 of the Criminal Code justify it, the administrative authority shall notify the persons mentioned in 1 of this I the electronic addresses of the services of communication to the public online that contravenes the provisions of this article, to which these persons must prevent access without delay. 'A decree sets the terms of application of the preceding paragraph, in particular those according to which the additional costs resulting from the obligations borne by operators are compensated, if necessary. '; 2 ° In the last paragraph of the same 7 and in the first paragraph of 1 of VI, the words: 'and fifth' are replaced by the words: ', fifth and seventh'. II. - The I comes into force six months from the publication of the decree provided for in the sixth paragraph of 7 of I of Article 6 of Law No. 2004-575 of 21 June 2004 for confidence in the digital economy and, at the latest, at the expiration of one year from the publication of this law.

Déclaration des Droits de l'Homme et du citoyen de 1789 – Article 10 : Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi.	Declaration of the Rights of Man and of the Citizen – Article 10: No one may be disturbed for his opinions, even religious ones, provided that their manifestation does not trouble the public order established by the law.
Déclaration des Droits de l'Homme et du citoyen de 1789 – Article 11 : La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi.	Declaration of the Rights of Man and of the Citizen – Article 11: The free communication of ideas and opinions is one of the most precious of the Rights of the Man. Every citizen may, accordingly, speak, write, and print freely, but shall be responsible for such violations of this freedom as shall be defined by law.
Loi du 29 juillet 1881 sur la liberté de la presse - Article 41 : Ne donneront ouverture à aucune action les discours tenus dans le sein de l'Assemblée nationale ou du Sénat ainsi que les rapports ou toute autre pièce imprimée par ordre de l'une de ces deux assemblées. Ne donnera lieu à aucune action le compte rendu des séances publiques des assemblées visées à l'alinéa ci-dessus fait de bonne foi dans les journaux. Ne donneront lieu à aucune action en diffamation, injure ou outrage ni les propos tenus ou les écrits produits devant une commission d'enquête créée, en leur sein, par l'Assemblée nationale ou le Sénat, par la personne tenue d'y déposer, sauf s'ils sont étrangers à l'objet de l'enquête, ni le compte rendu fidèle des réunions publiques de cette commission fait de bonne foi. Ne donneront lieu à aucune action en diffamation, injure ou outrage, ni le compte rendu fidèle fait de bonne foi des débats judiciaires, ni les discours prononcés ou les écrits produits devant les tribunaux. Pourront néanmoins les juges, saisis de la cause et statuant sur le fond, prononcer la suppression des discours injurieux,	Law on Freedom of press of 29 July 1881 – Article 41: Speeches made in the National Assembly or the Senate as well as reports or any other document printed by order of one of these two assemblies will not give rise to any action. The minutes of the public meetings of the assemblies referred to in the above paragraph made in good faith in the newspapers will not give rise to any action. Will not give rise to any action for defamation, insult or contempt or the words made or the writings produced before a commission of inquiry created, within them, by the National Assembly or the Senate, by the person required to testify there, unless they are foreign to the object of the investigation, nor the faithful report of the public meetings of this commission made in good faith. Will not give rise to any action for defamation, insult or contempt, nor the faithful account made in good faith of the legal proceedings, nor the speeches delivered, or the writings produced before the courts.

outrageants ou diffamatoires, et condamner qui il appartiendra à des dommages-intérêts. Pourront toutefois les faits diffamatoires étrangers à la cause donner ouverture, soit à l'action publique, soit à l'action civile des parties, lorsque ces actions leur auront été réservées par les tribunaux, et, dans tous les cas, à l'action civile des tiers.	However, the judges, seized of the case and ruling on the merits, may order the suppression of insulting, outrageous or defamatory speeches, and order that it belongs to them for damages. However, defamatory facts unrelated to the case may give rise either to public action or to civil action by the parties, when these actions have been reserved for them by the courts, and, in all cases, to action third parties.
LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme – Article 6 : I.-Après l'article 421-2-4 du code pénal, il est inséré un article 421-2-6 ainsi rédigé : 'Article 421-2-6.-I.-Constitue un acte de terrorisme le fait de préparer la commission d'une des infractions mentionnées au II, dès lors que la préparation de ladite infraction est intentionnellement en relation avec une entreprise individuelle ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur et qu'elle est caractérisée par : '1° Le fait de détenir, de rechercher, de se procurer ou de fabriquer des objets ou des substances de nature à créer un danger pour autrui ; '2° Et l'un des autres faits matériels suivants : a) Recueillir des renseignements sur des lieux ou des personnes permettant de mener une action dans ces lieux ou de porter atteinte à ces personnes ou exercer une surveillance sur ces lieux ou ces personnes ; b) S'entraîner ou se former au maniement des armes ou à toute forme de combat, à la fabrication ou à l'utilisation de substances explosives, incendiaires, nucléaires, radiologiques, biologiques ou chimiques ou au pilotage d'aéronefs ou à la conduite de navires ; c) Consulter habituellement un ou plusieurs	Law n ° 2014-1353 of 13 November 2014 strengthening the provisions related to the fight against terrorism - Article 6: I.- After article 421-2-4 of the penal code, an article 421-2-6 is inserted as follows: 'Article 421-2-6.-I. Constitute an act of terrorism the fact of preparing the commission of one of the offenses mentioned in II, since the preparation of said offense is intentionally in relation to an individual business with the aim of seriously disturb public order by intimidation or terror and is characterised by: 1 ° The fact of holding, researching, obtaining or manufacturing objects or substances likely to create a danger for others; 2 ° And one of the following other material facts: a) Gather information on places or persons enabling action to be taken in these places or to damage them, or exercise surveillance on these places or persons; b) To train or train in the handling of weapons or in any form of combat, in the manufacture or use of explosive, incendiary, nuclear, radiological, biological or chemical substances or in the piloting of aircraft or in the operation of ships;

services de communication au public en ligne ou détenir des documents provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie ; d) Avoir séjourné à l'étranger sur un théâtre d'opérations de groupements terroristes.	c) Usually consult one or more public communication services online or hold documents directly provoking or praising terrorist acts; d) Having stayed abroad in a theatre of operations of terrorist groups.
LOI n° 2005-842 du 26 juillet 2005 pour la confiance et la modernisation de l'économie – Article 9.I : I. - L'article L. 225-102-1 du code de commerce est ainsi modifié : 1° Après le deuxième alinéa, il est inséré un alinéa ainsi rédigé : 'Ce rapport décrit en les distinguant les éléments fixes, variables et exceptionnels composant ces rémunérations et avantages ainsi que les critères en application desquels ils ont été calculés ou les circonstances en vertu desquelles ils ont été établis. Il indique également les engagements de toutes natures, pris par la société au bénéfice de ses mandataires sociaux, correspondant à des éléments de rémunération, des indemnités ou des avantages dus ou susceptibles d'être dus à raison de la prise, de la cessation ou du changement de ces fonctions ou postérieurement à celles-ci. L'information donnée à ce titre doit préciser les modalités de détermination de ces engagements. Hormis les cas de bonne foi, les versements effectués et les engagements pris en méconnaissance des dispositions du présent alinéa peuvent être annulés.' ; 2° Après le quatrième alinéa, il est inséré un alinéa ainsi rédigé : 'Les dispositions des deux derniers alinéas de l'article L. 225-102 sont applicables aux informations visées au présent article.'	Law n ° 2005-842 of 26 July 2005 for the modernisation of the economy - Article 9.I: I- Article L. 225-102-1 of the Commercial Code is amended as follows: 1 ° After the second paragraph, the following paragraph is inserted: 'This report describes, by distinguishing between the fixed, variable and exceptional elements making up this compensation and benefits, as well as the criteria according to which they were calculated or the circumstances under which they were established. It also indicates the commitments of all kinds, taken by the company for the benefit of its corporate officers, corresponding to elements of remuneration, indemnities or benefits due or likely to be due to the taking, termination or change of these functions or subsequent to them. The information given in this respect must specify the methods for determining these commitments. Except in cases of good faith, payments made and commitments made in violation of the provisions of this paragraph may be cancelled.'; 2 ° After the fourth paragraph, the following paragraph is inserted: 'The provisions of the last two paragraphs of article L. 225-102 are applicable to the information referred to in this article.';

Bibliography

English titles

Legislation

Loppsi 2 Law No. 2011-267 of 14 March 2011 (Law of Orientation and Programming for the Performance of Internal Security)

French Data Protection Act

LCEN law, 21 June 2004

European Convention on Human Rights

The International Covenant on Civil and Political Rights, 1966

United Nations Universal Declaration of Human Rights (UDHR)

General Data Protection Regulation, 27 April 2016

Reports

Council of Europe, 'Comparative study on blocking, filtering and take-down of illegal internet content', 20 December 2015

Digital resources

Boring N, 'Limits on Freedom of Expression: France' (*Library of Congress,* June 2019) <https://www.loc.gov/law/help/freedom-expression/france.php)> accessed 1 March 2020

The Avalon Project <https://avalon.law.yale.edu/18th_century/rightsof.asp

https://www.echr.coe.int/Documents/Convention_ENG.pdf.

https://freedomhouse.org/sites/default/files/resources/FOTN%202015_France.pdf

Weber A, 'FALQs: Freedom of Speech in France' (27 March 2015) https://blogs.loc.gov/law/2015/03/falqs- freedom-of-speech-in-france/ accessed 1 March 2020

(https://www.vie-publique.fr/eclairage/24108-fausses-nouvelles-manipulation-comment-lutter-contre-les-fake-news).

Case law

De Haes and Gijsels v. Belgium, ECHR, (1997), No 19983/92

Morice v. France, Grand Chamber decision, ECHR, (2015)

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014), Court of Justice of European Union

Handyside v. United Kingdom (1976), ECHR

Von Hannover v. Germany (2004), ECHR

French titles

Legislation

Loi du 9 décembre 1905 concernant la séparation des Eglises et de l'Etat.

LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure

Déclaration des Droits de l'Homme et du citoyen de 1789

Loi du 29 juillet 1881 sur la liberté de la presse

LOI n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

LOI n° 2005-842 du 26 juillet 2005 pour la confiance et la modernisation de l'économie

Loppsi loi de 14 mars 2011: Décret No. 2015-125 5 février 2015

Code penal (Criminal Code)

Article 6-1, Created by law n°2014-1353 of 13 November 2014 - Article 12

Decree-Law of 23 October 1935

Decree no. 2015-253 of 4 March 2015

French Data Protection Act of 6 January 1978

Reports

'Nouveaux cahiers du conseil constitutionnel n° 36 - (dossier : la liberté d'expression et de communication) - juin 2012 '

Books

Barb A and Lacorne D, Les politiques du blasphème (2018)

A. Le Pouriets, L'encadrement juridique de la liberté d'expression en France,

Periodicals

La gazette du Palais (5 November 2019)

Les Petites Fiches by Lextenso, *La liberté d'expression protectrice des salariés lanceurs d'alerte de bonne foi* (17 novembre 2016)

Petites affiches, n°120 du 17 juin 2015, page 4

Digital resources

Réforme de la loi de 1881 : une nouvelle atteinte à la liberté de la presse, collective work, (2 July 2019) <https://www.liberation.fr/debats/2019/07/02/reforme-de-la-loi-de-1881-une-nouvelle-atteinte-a-la-liberte-de-la-presse_1737506>

https://www.lemondepolitique.fr/cours/libertespubliques/libertes/liberte_expression.html

http://www.regioneurope-apf.eu/wp/wp-content/uploads/2015/10/2015.09.24-Lencadrement-juridique-de-la-liberte%CC%81-dexpression-en-France-Intervention-de-Le-Pourhiet.pdf

https://www.conseil-constitutionnel.fr/decision/2011/2011625DC.htm

(https://www.cidj.com/vie-quotidienne/justice/liberte-d-expression-sur-le-web-limites-et-sanctions).

https://www.numerama.com/politique/145766-le-conseil-detat-valide-le-blocage-sans-juge-de-sites-internet.html.

(https://fr.reuters.com/article/topNews/idFRKBN1XU17K).

(https://fr.wikipedia.org/wiki/Filtrage_d%27Internet).

(https://www.journaldunet.fr/management/guide-du-management/1201587-internet-au-travail-ce-qu-il- faut-savoir/

Jean-François Sacré 'Le CSA veut réguler les réseaux sociaux ' (5 February 2020) <https://www.lecho.be/entreprises/media-marketing/le-csa-veut-reguler-les-reseaux-sociaux/10205928.html>

Case law

CA Paris, 11 March 1991 and 18 February 1992: Légipresse no. 95, page 112)

Cass. ass. plen., 25 Oct. 2019, No. 17-86605

The State Council, 15 February 2016

TGI Paris, 17th c., Jan. 9, 1992: Gaz. Pal. 92-1, 182

The decision No. 2011-625 DC of 10 March 2011 of the Constitutional Council

ELSA Germany

Contributors

National Coordinator

André Looks

National Academic Coordinator

André Looks

National Researchers

Daniel Hauck

Jan Schillmöller

Julian Pascal Beier

Said Ramadan Sadic

Simon Graf

National Academic Supervisor

Prof. Dr. Linda Kuschel, LL.M.

Prof. Dr. Markus Kotzur, LL.M.

PD. Mag. Dr. Matthias C. Kettemann, LL.M.

Prof. Dr. Wolfgang Schulz

Introduction

The Internet becomes more and more important in our society. In Germany it has a major influence on the life of nearly everyone. At the same time, the internet is not at a standstill, like our society it continually. Because of that, it is very difficult and yet so important to find appropriate and contemporary rules to regulate the internet. Recent issues that emerge when it comes to internet censorship are the questions about the specific legal requirements under which internet content can be filtered or blocked and about the fine line between the legal take down of unlawful actions like hate speech or cyber-racism and the issue of over blocking.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

Freedom of expression has the status of a basic right. Article 5 of the German Constitution (Grundgesetz - GG) guarantees and secures it in its first section in the form of speech, writing and pictures but also the freedom of press and reporting. The Freedom of Expression applies not only to Germans but also to foreign citizens (*Jedermanngrundrecht*).[596] In the third section of Article 5 GG the freedom of art and the freedom of science are guaranteed. They are, however, classified as specific guarantees, not as particular cases of the Freedom of Expression.[597] The Freedom of Expression serves two functions: Mainly it is a defensive right, which means that it protects people against the state in a subjective function (*status negativus*).[598] In comparison to this, basic rights form the Right to participate and the duty requires action imposed on the state (*status positivus*).[599] But there is also an objective function as the basic Rights form a part of the objective system of values.[600] The latter results in an influence on the civil law as it has to be interpreted in the light of the Freedom of Expression, therefore there is an indirect horisontal effect that comes from the basic right to freedom of expression.[601] The Freedom of Expression includes primarily the

596 Wendt, von Münch/Kunig, GG (6th edn, C.H.BECK 2012) Article 5, recital 4.

597 Oliver Jouanjan, *Freedom of Expression in the Federal Republic of Germany,* (Indiana Law Journal: Vol. 84, 2009), 867, 868 <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1126&context=ilj> accessed 5 February 2020.

598 BVerfG - 1 BvR 400/51.

599 Voßkuhle, Kaiser, Grundwissen - Öffentliches Recht: Funktionen der Grundrechte, JuS 2011, 411.

600 ibid, recital 26.

601 ibid, recital 27.

Right to express opinions.[602] Article 5 GG includes a broad term of opinion, which are defined as assertions that are characterised by assessments and statements.[603] Declarations of fact are protected only to the extent that they promote the formation of opinion.[604] There also is a negative freedom of expression, which forms the right to withhold an opinion.[605] There is a fine line when it comes to the truthfulness of the expression. On the one hand false information is not worthy of being protected as long as it does not support the formation of opinion.[606] For that reason, abusive criticism must be subordinate to the protection of honour, when it mainly serves the purpose to defame people instead of dealing with the discussed topic objectively.[607] On the other hand the requirement of truth should not discourage the speaker from expressing his opinions out of fear of legal consequences.[608]

1.1. Differentiation between legal restrictions and censorship

The first section of Article 5 GG states in its third sentence that there shall be no censorship. This does not create a fundamental right.[609] It rather implicates a restriction on potential restrictions on the Freedom of Expression (*Schranken-Schranke*).[610] The second section of Article 5 GG determines under which circumstances these restrictions are possible. It is a guideline for legal limitations on the rights named in Article 5, Section 1 GG. Section 2 of Article 5 GG names the protection of minors, the right to honour and reputation as well as the provision of general laws as limits to the Freedom of Expression. These general laws are characterised in a way that they do not restrict a specific opinion or information directly.[611] They rather affect opinions and/or information indirectly while protecting another legal asset.[612] This creates a qualified legal reservation as restrictions are dependent on above-mentioned purposes. There are several legal norms that limit the Freedom of Expression legally, for example Section 826 of the German Civil Code (Bürgerliches Gesetzbuch - BGB) or

602 BVerfG - 1 BvR 1376/79; Schemmer, BeckOK Grundgesetz (42. Edn, C.H.BECK 01.12.2019) Article 5, recital 6.
603 Schemmer, BeckOK Grundgesetz (42. Edn, C.H.BECK 01.12.2019) Article 5, recital 4.
604 ibid.
605 Oliver Jouanjan, *Freedom of Expression in the Federal Republic of Germany,* (Indiana Law Journal: Vol. 84, 2009), 867, 873 <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1126&context=ilj> accessed 5 February 2020.
606 BVerfG - 1 BvR 23/94; 1 BvR 1555/88.
607 BVerfG - 1 BvR 1476/91.
608 BVerfG - 1 BvR 23/94; 1 BvR 1555/88.
609 ibid 867.
610 ibid.
611 Von der Decken, Schmidt-Bleibtreu/Hofmann/Hennecke, GG (14th edn, Carl Heymanns 2017) Article 5, recital 35.
612 Ibid; Schemmer, BeckOK Grundgesetz (42. Edn, C.H.BECK 01.12.2019) Article 5, recital 99.

Section 185 of the German Criminal Code (Strafgesetzbuch - StGB).[613] To prevent inordinate limitations the Federal Constitutional Court (*Bundesverfassungsgericht*) stated that there is an interaction (*Wechselwirkung*) between the legal limitation itself and the affected right as a certain form of relationship in a way that the law and the Freedom of Expression restrict each other instead of an unilateral restriction.[614] The freedom of art and the freedom of science named in the third section of Article 5 GG are not included in the qualified restriction of Article 5, Subsection 2 GG.[615] However, this does not result in an unlimited freedom, as the freedom of art and the sphere of personality have to be weighed if there is a conflict between them.[616] In summary, censorship is prohibited in Germany according to Article 5, Subsection 1, Sentence 3 GG, which functions as a protection against disproportionate limitations on the Freedom of Expression. But there are still various opportunities to limit the freedom of expression, if this freedom collides with an interest on constitutional level.

1.2. The Right to Information

Article 5, Subsection 1, Sentence 1 GG also contains the Right to Information, which serves the individual freedom and the democratic principle in Germany.[617] It is a basic right, which holds a *status negativus* against the state.[618] It does not obligate the state to any actions like providing certain information or sources.[619] There are numerous legal regulations in place to give concrete form to the Right to Information. Most importantly there is the Freedom of Information Act (*Informationsfreiheitsgesetz - IFG*) on federal level, which came into force on 1 January 2006 and has the purpose to guarantee the civil right effectively, to support the democratic formation of opinion and to improve the monitoring of state activity.[620] Furthermore, 13 out of 16 federal states and several municipalities passed separate IFG's. In addition, there are, for example, the Environmental Information Act (*Umweltinformationsgesetz - UIG*) or the Consumer Information Act (*Verbraucherinformationsgesetz - VIG*), which concretise the right to information in certain areas. The right to information

613 Von der Decken, Schmidt-Bleibtreu/Hofmann/Hennecke, GG (14th edn, Carl Heymanns 2017) Article 5, recital 35.
614 BVerfG, - 1 BvR 400/51; Schemmer, BeckOK Grundgesetz (42. Edn, C.H.BECK 01.12.2019) Article 5, recital 100.
615 BVerfG -- 1 BvR 435/68.
616 ibid.
617 Wendt, von Münch/Kunig, GG (6th edn, C.H.BECK 2012) Article 5, recital 22.
618 Von der Decken, Schmidt-Bleibtreu/Hofmann/Hennecke, GG (14th edn, Carl Heymanns 2017) Article 5, recital 15.
619 ibid.
620 Schoch, Schoch IFG, § 1, recital 9.

remains subject to the legal requirements of the second section of Article 5 GG.[621] As a result, it is possible to pass general laws that limit the Right to Information. The most relevant legal restrictions are the Sections 3-6 IFG. These provisions state that the Right to Information can be limited when it stands against public interests (Section 3 IFG), the decision making process of authorities (Section 4 IFG), the protection of personal data (Section 5 IFG) or business and trade secrets/intellectual property (Section 6 IFG).[622] There are, of course, various other provisions in different special laws, which take precedence over the provisions of the IFG.[623]

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

The German legislator has enacted some specific laws to regulate the sensitive issue of blocking and takedown of internet content. The following is an overview of German legislation, the type of regulations and non-legal regulations.

2.1. Legislation specifically targeting blocking and taking down of content on the internet

The services of telemedia and the general framework of it are regulated in the Telemedia Act. The Telemedia Act was enacted on 26 February 2007 and went into effect on 1 March in the same year.[624] According to Section 1 Subsection 1 Sentence 1 of the Telemedia Act, telemedia is defined as each electronic information- and communication service, which is not a telecommunication service or a broadcast. This law was primarily enacted to unify the legal regulations with regard to the internet. A further aim of the Telemedia Act is the continuation of the implementation of the European E-Commerce Directive (Directive 2000/31/EC), which already began in the Tele Services Act and the State Media Service Treaty.[625] In his legal framework it has in Section 7

621 Schemmer, BeckOK Grundgesetz (42. Edn, C.H.BECK 01.12.2019) Article 5, recital 36.

622 Federal Ministry of the Interior, Building and Community, 'Informationsfreiheitsgesetz' <https://www.bmi.bund.de/DE/themen/moderne-verwaltung/open-government/informationsfreiheitsgesetz/informationsfreiheitsgesetz-node.html> accessed 7 February 2020.

623 ibid.

624 Federal Law Gazette from the year 2007 Part I Nr. 6, published in Bonn on 28 February 2007, Article 1 and 5; <www.bgbl.de/xaver/bgbl/stArticlexav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl107s0179.pdf>. accessed 2 February 2020.

625 Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG <https://web.archive.org/web/20060616035040/http://www.bmwi.de/BMWi/Redaktion/PDF/M-O/elgvg-elektronischer-gesch_C3_A4ftsverkehr-

Subsection 3 and 4 regulations about blocking and taking down of content on the internet. Furthermore, in view of hate speech, verbal insults and incitement of masses to hatred on social media, the German legislator enacted the Network Enforcement Act on 1 September 2017 to improve criminal prosecution in social networks.[626] The Network Enforcement Act went into effect on 1 October 2017.[627] It is the most detailed law on regulations of blocking or taking down internet content in social networks. It regulates in his Section 3 Subsection 2 the issue of blocking and taking down of content on social networks. Social media is defined in Section 1 Subsection 1 Sentence 1 in the Network Enforcement Act as tele media services which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public. Accordingly, the issue of blocking and taking down of content on the Internet is not regulated in one piece, but is scattered across several different types of laws.

2.2. Non-specific Regulations

Besides the legal regulations mentioned above, there are some non-specific regulations of the issue. The Federal States have ratified the Broadcast State Treaty, and how the name suggests it was initially intended only for broadcasting. But in March 2007 they added telemedia services to the treaty. The treaty regulates the areas of competences of the Federal States, sets basic principles and extra regulations about telemedia services. On the basis of such treaties the federal states commit themselves to a common approach with regard to a certain matter, especially with regard to the legislation of a matter where a unified approach is useful.[628] From a legal point of view, once the treaties have been approved by the Federal State Parliaments through an approval law, they have the status of a Federal State law.[629] The last amendment of the Broadcast State Treaty came into effect in May 2019.[630] But the Federal States have agreed on a

vereinheitlichungsgesetz,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf>, page 14, accessed 1 March 2020.

626 Federal Law Gazette from the year 2017 Part I Nr. 61, published in Bonn on 7. September 2017, Article <www.bgbl.de/xaver/bgbl/stArticlexav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3352.pdf.> accessed on 2 February 2020.

627 Federal Law Gazette Vintage 2017 Part I Nr. 61, published in Bonn on 7. September 2017, Article 3 <www.bgbl.de/xaver/bgbl/stArticlexav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3352.pdf.> accessed on 2 February 2020.

628 Aktueller Begriff, Staatsverträge zwischen den Bundesländern <https://www.bundestag.de/resource/blob/190052/424c9d512ff446a6aeadebf8a60725ee/staatsvertraege_zwischen_den_bundeslaendern-data.pdf> accessed on 1 March 2020.

629 ibid.

630 The Broadcast State Treaty in the version of his 22'th amendment, <https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Rundfunkstaatsvertrag_RStV.pdf> accessed on 6 February 2020.

new form of treaty. They have ratified the Media State Treaty, which will replace the Broadcast State Treaty, and it is planned that it comes into effect in September 2020. The Media State Treaty contains detailed regulations on telemedia services, especially for internet intermediaries such as Google, Facebook etc. But this treaty does not replace the specific laws on blocking and taking down of content on the internet. In addition to these treaties as non-parliamentary regulations, the Federal Ministry of the Interior has banned an association that operates a journalistic website on the basis of a non-specific law, namely Section 3 of the Association Act. With the ban against the association the Federal Ministry of Interior also banned the activities of the association owned website.[631] This is a very rare and extraordinary way to deactivate a website.

2.3. Cases related to blocking and takedown of internet content in which Germany has been a party

It is very rare that the state itself blocks or takes down Internet content, as it does not operate a platform where users can express their opinions or post other content. But state authorities may order platform operators to take down or block content with judicial orders based on the relevant law. Nevertheless, most cases about blocking or taking down internet content are cases between the users and the internet service providers in the civil courts. In spite of this, the Federal Ministry of Interior banned in the year 2017 an association named 'linksunten.indymedia' which operates a website with the same name.[632] This website was operated under the open-posting-principle, which means that the website has no specific editorial staff, but some rules of conduct for the use of the website, in this way it is similar to Facebook.[633] A user can leave comments or express his opinion about other topics. Together with this banning order the website was banned too. This invited a controversial discussion about freedom of expression and press. From a legal perspective it is interesting that the ban is based on association law instead of specific law about blocking or takedown of internet content. The decisive question has been whether the organisation 'linksunten.indymedia' is an association or not, because the organisation was never established officially. That is why the people behind the organisation have

631 Announcement of an association ban against „linksunten.indymedia" from 14 August 2017 by the Federal Ministry of the Interior, BAnz AT 25 August 2017 B1 <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2017/verbotsverfuegung-linksunten.pdf?__blob=publicationFile&v=1> accessed on 10 February 2020.

632 ibid.

633 David Werdermann and John page Thurn in <https://verfassungsblog.de/medienverbote-leicht-gemacht/> accessed 10 February 2020.

taken legal actions as individuals instead of representatives of an association.[634] The Federal Administrative Court decided that the organisation was an association, but did not review the ban because of the inadmissibility of the individual legal actions.[635] According to Section 2 Subsection 1 of the Associations Act, an association, irrespective of its legal form, is any association in which a majority of natural or legal persons have voluntarily joined together for a longer period of time for a common purpose and subjected themselves to an organised decision-making process. Another legal issue is the principle of specific law that supersedes general law (*lex specialis derogat legi generali*), in particular the Telemedia Act, over association law. In accordance with the Broadcast State Treaty, the supervision of tele media services is the responsibility of the federal states. The main argument that a federal authority was acting here instead of a federal state authority is that the Telemedia Act is a law only for individual punishable contents, whereas the law on associations is for unlawful associations.[636] Furthermore, the ban should not be a media ban, but a ban on associations.[637] The people behind 'linksunten.indymedia' therefore announced a constitutional complaint.[638] It remains to be seen how this case will develop.

2.4. List of legislation and how it regulates the issue

According to Section 7 Subsection 3 of the Telemedia Act, a telemedia provider is obliged under general law to take down or block content on his platform due to a court or order of the authorities. It is not relevant whether the provider is responsible for the content or not. Section 7 Subsection 4 of the Telemedia Act sets the obligation on the provider to block content if it violates copyrights to prevent repeats of this violation. But the blocking of the content must be reasonable and proportionate. Special for social media contents Section 3 of Network Enforcement Act delegates monitoring about unlawful contents to the social media providers by setting the obligation to establish an own complaint mechanism for the users. According to Section 3 Association Act, an association can be banned if it acts against the criminal law, the constitutional order or the understanding among the nations. This is not a specific law to take down or block internet content but the Federal Ministry of Interior has used it to deactivate a website operated by an association. Since the Association Act only

634 Daniel Laufer in <https://netzpolitik.org/2020/linksunten-indymedia-bleibt-verboten/> accessed on February 2020.

635 Press release of the Federal Administrative Court from 30 January 2020, reference Nr. 05/2020, <https://www.bverwg.de/pm/2020/5> accessed 10 February 2020.

636 David Werdermann and John page Thurn in <https://verfassungsblog.de/medienverbote-leicht-gemacht/> accessed 10 February 2020.

637 ibid.

638 Daniel Laufer in <https://netzpolitik.org/2020/linksunten-indymedia-bleibt-verboten/> accessed 10 February 2020.

applies if an association exists and the Telemedia Act stands as a special law for telemedia services, the relationship between these laws must be clarified.

2.5. Policy papers and proposals

The Federal Ministry of Justice and Consumer Protection published two draft laws to improve and develop the Network Enforcement Act and the Telemedia Act. The first draft law was published on 19 December 2019 and provides for a fight against right-wing extremism and hate crimes, which can be seen in the brutalisation of communication via social media.[639] This draft law was also adopted by the Federal Cabinet on 19 February 2020.[640] Very disputed are new regulations on Section 15a of the Telemedia Act and Section 10 Subsection 1 of the Federal Criminal Police Agency Act. In the draft, the Telemedia Act provides in Section 15a that social media providers should handing out passwords of accounts to the Federal Criminal Police Agency and Section 10 Subsection 1 of the Federal Criminal Police Agency Act provides that the Federal Criminal Police Agency should save contents, IP-addresses and other dates about users who supposedly published unlawful content.[641] The second draft law was published on 29 January 2020 and provides primarily the same aim of the first draft, but with special features.[642] Remarkable are Section 2 Subsection 2 Nr. 2 and 13 of the second draft. In Nr. 2 it is provided that the social media provider should report about his automatised mechanisms like artificial intelligence to detect unlawful content. In Nr. 13 of the same draft it is provided that the social media provider should report which user groups frequently attract attention by publishing illegal content. From September 2020, the Broadcast State is to be replaced by a Media State Treaty, which is to contain new regulations for Internet services such as Internet intermediaries.[643]

---

639 Draft of the Federal Ministry of Justice and Consumer Protection from 19 December 2019, Page 1 <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_BekaempfungHatespeech.pdf?__blob=publicationFile&v=1> accessed 9 February 2020.

640 Bundesministerium der Justiz und für Verbraucherschutz, Gesetzespaket gegen Rechtsextremismus und Hasskriminalität <https://www.bmjv.de/SharedDocs/Artikel/DE/2020/021920_Kabinett_Bekaempfung_Rechtsextremismus_Hasskriminalitaet.html> accessed 1 March 2020.

641 CR-online.de Blog, Seid wachsam, Bürgerrechtler – BMJV verwirrt durch zwei separate Entwürfe zum NetzD <https://www.cr-online.de/blog/2020/01/29/seid-wachsam-buergerrechtler-bmjv-verwirrt-durch-zwei-seperate-entwuerfe-zum-netzdg/> accessed 9 February 2020; Draft of the Federal Ministry of Justice and Consumer Protection from 19 December 2019, Pages 7 - 9, <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_BekaempfungHatespeech.pdf?__blob=publicationFile&v=1> accessed 9 February 2020.

642 Draft of the Federal Ministry of Justice and Consumer Protection from 29 January 2020, Page 1 <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_NetzDGAendG.pdf?__blob=publicationFile&v=3> accessed on 9 February 2020.

643 Draft of the Media State Treaty from 5 December 2019,

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

In Germany, internet content can basically only be blocked or taken down for one reason, namely if it is unlawful. Section 7 Subsection 3 Telemedia Act stipulates the blocking or taking down of internet content if it is ordered by a state authority or a court according to the general laws. Another reason for taking measures against an internet content is, according to Section 7 Subsection 4 of Telemedia Act, the violation of a Copyright. When a telemedia service has been used by a user to infringe the copyright of another person, and the holder of that right has no other means of remedying the infringement of his right, the right holder may require the service provider to block the content. However, this must be claimed by the person affected by the copyright infringement. The Network Enforcement Act pursues the intention of regulating internet content in the context of social media. According to Section 1 Subsection 3 of the Network Enforcement Act, unlawful content in this context is that which violates certain norms of the Criminal Code. Finally, the Federal Ministry of the Interior deactivated a website also on the basis of the law on associations because its purposes and activities are contrary to criminal law and constitutional order.[644]

3.1. Which safeguards are in place to ensure a balance between censoring and freedom of expression?

In general, there is no special regulation to establish a balance between censorship and Freedom of Expression. In principle, a person affected by taking down or blocking internet content from private providers or from state authorities can go to court. Here, it is only relevant who censored the content. If it is censored by a state authority, the affected person has to take legal actions by the administrative court. If it is censored by a private tele media provider, the affected person has to take legal actions by the civil courts. This is not a very specific way of safeguarding internet contents, but a legal expert as a judge could review the dispute very accurately at the legal level. Only in the Network

<https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/ModStV_MStV_und_JMStV_2019-12-05_MPK.pdf> accessed 9 February 2020.

644 Announcement of an association ban against „linksunten.indymedia" from 14 August 2017 by the Federal Ministry of the Interior, BAnz AT 25 August 2017 B1 <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2017/verbotsverfuegung-linksunten.pdf?__blob=publicationFile&v=1> accessed on 10 February 2020; Announcement of a association ban against „Altermedia Deutschland" from 04. January 2016 by the Federal Ministry of the Interior, BAnz AT 27 January 2016 B1 <https://www.bundesanzeiger.de/ebanzwww/wexsservlet?session.sessionid=141f108870e40a3a47f5e3e183ffd5d8&page.navid=detailsearchlisttodetailsearchdetail&fts_search_list.selected=f498931aa30af58c&fts_search_list.destHistoryId=58304> accessed 6 February 2020.

Enforcement Act are some specific regulations which could be categorised as specific safeguards. In Section 2 of the Network Enforcement Act it is provided that the social media provider has to report of it is measures against unlawful content and its results in a very detailed way. In addition, the provider is obliged to apply an effective complaints procedure according to Section 3 Network Enforcement Act. Within the framework of this complaints procedure, the provider reviews whether illegal content is actually present. If carried out properly, this review can serve as a safeguard for Freedom of Expression. If the social media provider fails to comply with these and other obligations, a fine may be imposed on him in accordance with Section 4 of the Network Enforcement Act.

3.2. What is the process of judicial review of cases where content has been blocked or taken down from the internet? Does the review constitute effective protection of freedom of expression online?

If the content has been blocked or taken down by the state, the matter is a case for the Administrative Court.[645] In the case of an association ban, the Federal Administrative Court is the competent court of first instance. However, if a taking-down or blocking has been carried out on the basis of an order by a Federal State Authority, the normal Administrative Court of the Federal State concerned is competent. If the content was blocked or taken down by a private operator, the matter is a case for the civil court. For effective legal defence, an application for a temporary injunction is usually filed. This is done at the District Court. If no success is achieved there, an application is filed with the Higher District Court. If no success is achieved there either, a constitutional complaint can be filed with the Federal Constitutional Court.[646] According to civil court jurisdictions the contract between the user and the platform operator establishes protection duties in favour of the user, so that in this context the basic rights of the user, especially the freedom of expression, must be taken in account.[647] But on the other hand, the user must also take into account his or her obligations arising from the contract with the operator. The operator can specify these obligations by setting up rules of conduct and also enforce them by blocking the user account.[648] By way of legal action, the user can obtain a temporary

645 Press release of the Federal Administrative Court from 30 January 2020, file reference: Nr.5/2020.

646 BVerfG - 1 BvQ 42/19, http://www.bverfg.de/e/qk20190522_1bvq004219.html accessed on 01 March 2020.

647 District Court Frankfurt - 2-03 O 310/18 <https://www.rv.hessenrecht.hessen.de/bshe/document/LARE190005792> accessed on 6. February 2020.

648 OLG München - 18 W 1383/18 <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-23547?hl=true> accessed on 01 March 2020.

injunction or a judgement against the platform provider to restore the content.[649] At the end the review by a judge is very effective because of the detailed analysis of the content by a legal expert. But due to the ordinary legal action it could be a costly and time-consuming process. At the end of the ordinary legal action the complainant has the possibility to submit a constitutional complaint to the Federal Constitutional Court.

3.3. Compliance with the case law of the European Court of Human Rights

There are multiple important decisions of the European Court of Human Rights (ECtHR), which formed case law in the past. First, there is the case of *Ahmet Yildirim v. Turkey* (18 December 2012), in which the website of the applicant got blocked due to criminal proceedings against the owner of another website, who was accused of insulting the memory of Atatürk. The ECtHR Chamber stated that a limitation by the public authorities on the freedom of expression would only conform with Article 10 of the European Convention of Human Rights (ECHR), if it was prescribed by law, if it pursued at least one legitimate aim and if it was necessary in a certain public interest.[650] There has to be a strict legal framework in place as well, which regulates the scope of this limitation and guarantees the judicial review of any restriction.[651] In addition, a rule must be 'foreseeable', which means that it has to be formulated with a certain precision to qualify people to regulate their conduct.[652] In this case it was also pointed out that Article 10 ECHR guarantees the right to freedom of expression 'regardless of frontiers'.[653] Another important case is *Cengiz and Others v. Turkey* (1 December 2015). It deals with the blocking of access to YouTube and the problem of over blocking, which means the blocking of more content than the necessary amount.[654] It, again, emphasises the need of an legitimate goal and that the blocking, filtering or take down of any internet content must be necessary to achieve this legitimate goal.[655] All in all, it is a question of legitimacy, necessity and proportionality when it comes to restrictions on the right to freedom of

649 District Court Bamberg - 2 O 248/18, <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-26648?hl=true> accessed on 8. February 2020; OLG München - 18 U 1491/19Pre.

650 Application no. 3111/10 <https://hudoc.echr.coe.int/eng#{"itemid":["001-115705"]}> accessed 13 February 2020.

651 ibid.

652 ibid.

653 ibid.

654 ECJ - 48226/10 und 14027/11.

655 ibid.

expression on the internet in the form of filtering, blocking or take down of content.[656]

In Germany there is most importantly Section 7 Subsection 3 and 4 of the TeleMedia Act as a legal regulation regarding the removal of internet content. According to the official justification for Section 7 of the TeleMedia Act the obligations to remove or block the usage of information is only permitted, if it is regulated by law and happens on the basis of a judicial or administrative order.[657] This is to ensure a balance of interests in the particular case.[658] This provision must be interpreted in accordance with the EU directives.[659] On the one hand, this regulation follows the requirements of the case law of the ECtHR in a way that it prescribes a balance of interests in the particular case.[660] On the other hand, there is a possible evaluation contradiction between Subsection 2 and Subsection 3 as well as potential problems with the interpretation in accordance with the EU directives:[661] There should be no obligation for internet providers to monitor everything permanently, but at the same time there should be such obligations even without the requirement of any responsibility.[662] To solve this conflict, Subsection 3 must be restricted insofar as an obligation to remove unlawful content arises only if the provider has information about incidents.[663]

3.4. Relevant case law

Relevant case law in Germany regarding filtering or blocking internet content is existing in multiple variations. An important decision was the *Internet-Versteigerung II* (19 April 2007), which stated that providers on internet platforms, who were given notice of certain breaches, must not only block the respective offer instantly, but have to ensure that these breaches will not occur in the future as well.[664] The decision *Jugendgefährdende Medien bei eBay* (12 July 2007) discussed a similar case. The Federal Court of Justice (Bundesgerichtshof - BGH) stated in this decision that internet providers have the obligation to examine not only offers that are potentially harmful to youth but also have special obligations to examine the auctioneers who provided such offers in the past.[665] Another

656 ibid.
657 Hofmann/Volkmann, Spindler/Schuster, Recht der elektronischen Medien (4th edn, C.H.BECK 2019) § 7 TMG, recital 39.
658 ibid.
659 ibid, recital 37.
660 ibid, recital 39.
661 ibid, recital 40.
662 ibid.
663 ibid, recital 41.
664 BGH - I ZR 35/04.
665 BGH - I ZR 18/04.

important decision is from 27 March 2007. It deals with the possible liabilities of owners of opinion forums. The BGH made the decision that owners of such forums are responsible for content that violates another one's honour even when they know the identity of the author of this violation.[666] In addition, the injured might have an injunctive relief against the owner.[667] Furthermore, the BGH made clear that file-hosting services can bear liability, if they have information about people using their service in a way that violates copyright law, in the decision named *Alone in the Dark* from 12 July 2012.[668] Instead, providers have to take actions against those violations in a technical and economical reasonable extent.[669] Those actions may consist of word filters, but it was also stated that manual controls are generally reasonable and not excluded in principle.[670]

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In general, German public authorities do not have the possibility of blocking or taking down internet content on their own. They are reliant on participation of the Internet Service Providers. Nevertheless, they can instruct them to take down or block internet content with an administrative order. The authorities are responsible for surveillance of compliance with general laws such as the Telemedia Act. As a result of the Network Enforcement Act social media platforms have to provide a complaints mechanism for unlawful contents. The Network Enforcement Act as a specific legislation for social network platforms excludes platforms with journalistic or editorial content, platforms which enable individual communication or the dissemination of specific content and platforms with less than two million users. Social media is defined as telemedia service providers which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public. A complaint can be filed by any user or organisation. As part of the process the social media providers have the possibility to review the complained content and if necessary, take it down or block it. Primarily, the whole process is the responsibility and in the disposition of the social media provider. In case that the complainant is not satisfied with the decision of the social media provider, an online notification to the Federal

666 BGH - VI ZR 101/06.
667 ibid.
668 BGH - I ZR 18/11.
669 ibid.
670 Hühner, Anm. zu BGH, Urteil vom 12.07.2012 - I ZR 18/11, GRUR 2013, 373, 375.

Office of Justice is possible, because according to Section 3 Subsection 5 of the Network Enforcement Act the review process can be monitored by an authority mentioned in Section 4 of the Network Enforcement Act.[671] According to Section 4 Subsection 4 Sentence 1 of the Network Enforcement Act the Federal Office of Justice is one of these authorities. Additionally, a criminal charge based on a violation of national law can be filed with the police, the public prosecutor or the district court. The assessment of the complaints by the social media providers is based on the Network Enforcement Act at the one hand and the own community standards respectively rules of the platform providers at the other hand, for example Facebook's community rules and Twitter's rules and policies. Facebook has taken a two-step approach to review content that is reported through the 'Network Enforcement Act reporting form'.[672] First, they review the content about compliance with the community standards and if the result is positive, they review it about compliance with the Network Enforcement Act. The difference between a violation of the Network Enforcement Act and a violation of the community standards is a difference of the consequences. A breach of community standards leads to a worldwide take down of the content from the Facebook platform.[673] If the content only breaches regulations of the Network Enforcement Act, the content will only be blocked on the German Facebook platform.[674] In its transparency report for the first half of 2018, Facebook listed only the violations reported via the special form, but not those found via other means.[675] For this violation of the reporting obligation, which made the number of illegal contents appear artificially smaller, the responsible BfJ imposed a fine of 2 million euros.[676] Twitter also has two kinds of approach to complaining content similar to the approach of Facebook. But it offers different ways for law enforcement authorities and normal users. Users can only complain about content without the option of a specific request.[677] Law enforcement agencies can ask for a take down or for blocking of content. Either the content violates the internal rules of Twitter, then it would be taken down

671 Form for reporting to the Federal Office of Justice, <https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/NetzDG/Service/Formulare/Meldung/Formular_node.html> accessed 5 February 2020.

672 <https://www.facebook.com/help/285230728652028> under the topic 'What's the difference between NetzDG and Facebook's Community Standards?' accessed 31 January 2020.

673 ibid.

674 ibid.

675 Facebook, <https://fbnewsroomus.files.wordpress.com/2018/07/facebook_netzdg_juli_2018_deutsch-1.pdf>, accessed 28 February 2020.

676 BfJ, <https://www.bundesjustizamt.de/DE/Presse/Archiv/2019/20190702.html> accessed 28. February 2020.

677 Twitter report violation policy <https://help.twitter.com/en/rules-and-policies/twitter-report-violation> accessed 31 January 2020.

by Twitter worldwide.[678] Or it violates only national law, then Twitter would block it only in the boundaries of the affected country.[679] Additionally, according to Section 3 Subsection 6 Network Enforcement Act social media providers have the option to establish an institution of regulated self-regulation. According to the same section the requirements for the establishment of regulated self-regulation are mainly expertise and independence of the inspectors, briskness, transparency and accountability of the process, a merger of social media providers or other institutions and the opportunity for other providers especially social media providers to join the institution.

4.1. Safeguards for ensuring the protection of freedom of expression where self-regulation is applied

First of all, a complaint must be reasoned by the complainant, the content the complaint is about must be mentioned and the complainant has to give his contact information. After this, the social media provider asks the defendant about his view on the content. In parallel the social media provider forms it is own picture of the matter. In addition, Section 2 of the Network Enforcement Act sets the commandment to social media providers which get more than hundred complaints to publish half-yearly a detailed report about their complaint results, their complaint system, their measures to prevent unlawful activities on their platform and other similar points.

4.2. Grievance redressal mechanism

The whole complaint process including a possible grievance redressal mechanism is according to Section 3 Subsection 1 Network Enforcement Act in the disposition of the provider of social networks. The legislation gives the requirement that the process should be effective and transparent. But a grievance redressal mechanism is not dictated by law. Nevertheless, most social media providers put up the possibility to remove the disposal of the content if this was according to his opinion not justified. But if the social media provider does not remove the disposal, the complainant has only the option to bring this matter to the civil court.

678 Twitter law enforcement support <https://help.twitter.com/de/rules-and-policies/twitter-law-enforcement-support#16> accessed 31 January 2020.

679 ibid.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

As 'Right to be Forgotten' respectively the 'Right to Delete' is considered the idea of an 'digital eraser' that enables individuals to actively monitor and influence its data in the digital age.[680]

Since Germany is a member state of the European Union there is a right to be forgotten out of Article 17 of the General Data Protection Regulation (GDPR) which is directly applicable in Germany, following out of Article 288 TFEU.[681] But even before the GDPR came in to effect in 2018 the German legislation did know a corresponding right[682] (which was abolished due to the prohibition to repeat standards),[683] flanked by encouraging jurisdiction of the German Federal Constitutional Court.[684] Nonetheless the German Legislation has concretised the right granted in Article 17 GDPR based on Article 23 GDPR in Section 35 of the Federal Data Protection Act (*Bundesdatenschutzgesetz - BDSG*).[685] The first part of this analysis will examine this concretisation, while the following part will lay out constitutional safeguards in place to ensure this right.

5.1. Concretisation of Article 17 GDPR in Germany

The right to be forgotten can be regarded as one of the most important potential influences that can affect the procession of data.[686] Nevertheless the German legislator uses Section 35 BDSG to restrict this right further than it is possible based on Article 17 Subsection 3 GDPR. The right to be forgotten according to Article 17 GDPR is replaced by the right to restriction of processing pursuant to Article 18 GDPR if the data in question is processed automatically and can only be deleted by a disproportionately big effort (Section 35 Subsections 1 and 2 BDSG). Furthermore, the Right to be Forgotten is also suspended if deleting data would conflict with retention periods set by statute or contract (Section 35 Subsection 3 BDSG).

This restriction of the right to be forgotten has been based on Article 23 GDPR by the German legislator. Whether or not the restriction of Article 17 GDPR

680 Singer/Beck, Jura 2019, 125.
681 Roßnagel, DuD 2017, 277
682 §§ 20, 35 BDSG (old version).
683 ECJ - C-272/83; BeckOK DatenschutzR/Worms, BDSG § 35 recital 3 et seq.; HK-BDSG/Peuker § 35 recital.3.
684 BVerfG - 1 BvR 209/83; 1 BvR 370/07.
685 Bundestag-Drucksache 18/11325, page 105.
686 HK-BDSG/Peuker § 35 recital 1.

does comply with the possibilities of Article 23 GDPR enabled for member states is highly questionable.[687]

Article 23 GDPR opens the possibility for member states to restrict the rights granted in Article 17 GDPR only because of certain regulatory goals mentioned in this provision.[688] A regulatory goal relevant in this case could be Article 17 Subsection 1 lit. e GDPR which requires 'important objectives of general public interest of the Union or of a Member State'.[689] The prevention of disproportionally big effort could possibly be such an goal of general public interest, but the wording of Section 35 Subsection 1 BDSG seems to be too vague, creating a blanket clause which undermines the general intention of Article 17 GDPR, especially because non-public data processors are able to restrict the Right to be Forgotten too.[690] Also the official explanatory memorandum for Section 35 BDSG by the German legislators does not instance any examples of objectives of general public interest and just refers to Article 23 Subsection 1 GDPR in general to justify this restriction[691], so that it is not able to concretise the vague blanket clause created in Section 35 Subsection 1 BDSG.

In fact, the restriction in Section 35 Subsection 1 BDSG is identical to the German legislation before the GDPR came into force, (Sections 20 and 35 BDSG old version)[692] so that the intent of the European legislators to unify the data protection law and to overcome fragmented national legislation is undermined. [693]

5.2. Constitutional Safeguards

Data Protection regulations in Germany are based and protected by the 'Right to Informational Self-Determination' which the Federal Constitutional Court has derived out of the general right of privacy under Article 1 Subsection 1 (guarantee of human dignity) and Article 2 Subsection 2 (right to general freedom of action) of the German Basic Law.[694] This right prohibits the state power to unjustified collect and save personal data[695] and shall enable the citizen to decide alone over disclosure and procession of his personal data.[696] But not only public data processors are bound by this basic right. Because of the indirect

687 Paal/Pauly/Paal, BDSG § 35 recital 2.
688 HK-BDSG/Peuker § 35 recital 6.
689 Kühling/Buchner/Herbst, BDSG § 35 recital 16.
690 ibid.
691 Bundestag Drucksache 18/11325, page 105.
692 ibid.
693 Helfrich, ZD 2017, 97.
694 BVerfG - 1 BvR 209/83; Jarass/Pieroth/Jarass, GG Article 2 Abs. 1, recital 37.
695 Nolte, ZRP 2011, 236; BeckOK Grundgesetz/Lang, GG Article 2 recital 45.
696 Jarass/Pieroth/Jarass, GG Article 2 Abs. 1, recital. 42.

third-party effect, the German Constitutional Court awards to the basic rights in the Basic Law also private data processors can be held responsible,[697] e.g. through an injunctive relief based on Sections 823 Subsection 1 and 1004 analogue of the German Civil Code.[698]

This protection of privacy through the 'Right to Informational Self-Determination' was first established by the German Constitutional Court in his 'population census'-ruling in 1983, when automatic procession of data first came to the attention of the court.[699] But there are even older rulings which already indicated a related right (e.g. the 'micro census'-ruling in 1963).[700] Since then this right has gained in importance in the jurisdiction of the German Federal Constitutional Court,[701] with the result that even without European legislation on data protection the German constitution would demand that every citizen has a right to be forgotten concerning his personal data.[702] The German concept of informational self-determination was in its development and range inspired by the American concept of the right to privacy that has existed since 1890,[703] but in its doctrinal reason the German right is not only based on the 'Right to be let alone' as in America, furthermore it is strongly based directly on the guarantee of human dignity in Article 1 of the German Constitution.

Since there have been no clear majorities in the German parliament, so far, no explicit basic right to data protection could be established in the Basic Law. Unlike at a European level with Article 8 of the European Charter of Fundamental Rights, such a basic right was not introduced with the GDPR. For this reason, it is still necessary to resort to the general right of personality for further development of the law by judges in order to provide effective fundamental rights protection. In addition, a fixed fundamental right would be rigid and technical innovations would have to be constantly adapted.

The law of the European Charter of Fundamental Rights must be taken into account when interpreting national fundamental rights. Especially because the European Parliament derives the right from Article 8 ECHR, which as Union law is pursuant to Article 23 GG primarily applicable over national legislation (supremacy of Union law). Violations can also be brought directly before

697 BeckOK Grundgesetz/Lang, GG Article 2 recital 45; Maunz/Dürig/Di Fabio, GG Article 2 Abs. 1 recital 191.
698 BeckOGK/Spindler, BGB § 823 recital 189.
699 BVerfG - 1 BvR 209/83; BeckOK Grundgesetz/Lang, GG Article 2 recital 45.
700 BVerfG - 1 BvL 19/63.
701 Dreier/Dreier, 3. Auflage GG Article 2 Abs. 1 recital 79.
702 Nolte, ZRP 2011, 236.
703 Götting, GRUR Int 1995, 656.

national courts. Another form of the right of personality is the confidentiality of technological systems.

The federal constitutional court has just recently extended the options of legal protection in its 'Right to be Forgotten I and II'-rulings.[704] Even though there is no explicit basic right to privacy stated in the German constitution, the federal constitutional court accepted two constitutional complaints for a decision in which an infringement of Article 8 ECHR was complained of. Thereby widening the scope of its control functions beyond the basic rights of the German Basic Law to the European Charter of Human Rights in the event of a case which is fully determined by European Union Law.[705] In the contrary case the Federal Constitutional Court reviews cases that are not fully determined by European Union Law still only under the standards of the Basic Rights of the Basic Law – thus if the right to be forgotten is concerned under the standard of the right to informational self-determination, pursuant to Article 1 Subsection 1 and Article 2 Subsection 1 of the Basic Law. Although the case is fully determined by European Union Law, the Federal Constitutional Court now directly takes Article 8 ECHR into account.[706]

This decision was necessary in the eyes of the Federal Constitutional Court as there is no effective legal remedy in European Union Law for citizens to claim that their fundamental rights granted in the European Charter of Human Rights were violated in front of the Court of Justice of the European Union.[707] As Article 17 GDPR is European Union Law and fully harmonising, these recent decisions of the Federal Constitutional Court make it possible to not only claim a violation of Article 17 GDPR in front of national courts, who have to consider the rights of the Charter in their decision,[708] but also to challenge the decision of the court in front of the Federal Constitutional Court. Thereby the protection of privacy and the enforceability of the right to be forgotten is further ensured.

704 BVerfG - 1 BvR 16/13; 1 BvR 276/17.
705 Kühling, NJW 2020, 275.
706 Ibid.
707 https://www.lto.de/recht/hintergruende/h/bverfg-recht-auf- vergessen- europa-eugh-grundrechte-teil-2/, accessed 29. February 2020.
708 Ibid.

6. How does your country regulate the liability of internet intermediaries?

Internet intermediaries are considered as 'service providers that facilitate interaction on the internet between natural and legal persons'.[709] These service providers are liable under the regulation of the general law, which is clarified in Section 7 Subsection 1 Telemedia Act (*Telemediengesetz – TMG*). However, in the Sections 7 et seq. TMG their liability is privileged depending on the kind of service provided, as result of transposing Article 12-15 Directive 2000/31/EC into German Law.[710]

As general laws in this context can be considered especially Sections 823, 1004 (analogue) BGB, granting an injunction relief against e.g. violations of the general Right to Privacy,[711] but also Section 97 Subsection 1 Act on Copyright and Related Rights (*Urheberrechtsgesetz – UrhG*) and Section 14 Subsection 5 and Section 15 Subsection 4 Trademark Act (*Markengesetz – MarkenG*) against violations of intellectual property and Section 8 of the Law against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb – UWG*).[712]

The TMG makes a distinction between content providers (Section 7 TMG), access providers (Sections 8, 9 TMG) and host providers (Section 10 TMG) when regulating the liability of service providers.[713]

Content providers are not privileged for the publishing of proprietary content according to Section 7 Subsection 1 TMG. Also, the privileged status is omitted if foreign content is adopted as own content,[714] which is the case when the foreign content seems to be part of the providers online presence and/or the service provider has assumed responsibility for the selected information from an objective point of view.[715]

Pursuant to Sections 8 and 9 TMG access providers – those service providers which are giving access to third-party information (Section 8 TMG) or is transmitting foreign information (Section 9 TMG)[716] – are excluded from liability for damages.[717] Nevertheless the access provider stays responsible for deleting and blocking unlawful content, but only after a notification. As well as for

709 <https://www.coe.int/en/web/freedom-expression/internet- intermediaries>, accessed 9 February 2020.
710 BeckOK InfoMedienR/Paal, TMG § 7 recital 4.
711 Hoffmann, JuS 2017, 713.
712 BeckOK InfoMedienR/Paal, TMG § 7, recital 5.
713 Hoeren, Internetrecht, Page 555, recital 1158.
714 Spindler/Schuster El. Medien/Hoffmann/Volkmann, TMG § 7, recital. 14.
715 BGH - I ZR 166/07; jurisPK-Internetrecht/Roggenkamp/Stadler, Chapter 10, recital 86.
716 Hoeren, Internetrecht Page 555, recital 1158.
717 Ibid. Page 562, Recital 1180.

content and host providers there is no original obligation for investigation, pursuant to Section 7 Subsection 2 TMG.[718] This procedure is known as 'notice and take down'-procedure.[719]

Operations that are performed automatically and can be considered communication-like are completely excluded from any liability of the provider.[720] This is also clarified in Section 7 Subsection 3 TMG and a result of the secrecy of telecommunications granted in Article 10 Subsection 1 of the German Basic Law.[721]

Nonetheless the privileged status is revoked in the case of an access provider colluding with a user to commit any unlawful action (Section 8 Subsection 1 1st Sentence TMG). Condition for such a collusion though is a direct intent of the service provider.[722]

Section 10 TMG regulates the lability of the host provider. Those service providers who are storing and holding ready foreign information for using.[723] Host providers most prominently include social networks or e.g. blogs.[724] The liability of these service providers is excluded as long as they have no knowledge of the unlawful content processed by them. That means that they either need to have positive knowledge of the unlawful content or the presence of facts and circumstances that indicated an obvious unlawfulness.[725] Due to the high standards of knowledge a host provider has to have before he is obliged to act, they are comparable to access providers in their liability, de facto also only responsible for conducting a notice and take down-procedure.[726] Similar to the liability of access providers only compensation reliefs are excluded. The privileged status does not include injunction reliefs or criminal liability.[727]

However Section 10 TMG leads to the problem that the liability of host providers is dependent on the understanding of the term 'obvious unlawfulness'.[728] Furthermore such a provision can lead to the case that service providers are consciously reducing their control of content in order to not receive positive knowledge of unlawful content which could trigger their own

718 BeckOK InfoMedienR/Paal, TMG § 7 recital 49.
719 Hoffmann, JuS 2017, 715.
720 Spindler/Schuster El. Medien/Hoffmann/Volkmann, TMG § 8, recital 7.
721 BeckOK InfoMedienR/Paal, TMG § 7, recital 71.
722 JurisPK-Internetrecht/Roggenkamp/Stadler, Chapter 10, recital 154.
723 ibid. recital 61.
724 ibid. recital 233.
725 Hoeren, Internetrecht, Page 566, recital 1188.
726 Hoeren, Internetrecht, Page 368, recital 1191.
727 BGH - I ZR 139/08.
728 ibid.

liability.[729] This concern though is weekend by the fact, that the exclusion of liability is only removed by human knowledge, meaning that the knowledge of electronic safeguards or algorithms is not sufficient and the providers is not hindered of using such possibilities to pre-emptive search for unlawful content.[730] Furthermore, taking down or blocking unlawful content must even in the case of positive knowledge or obvious unlawfulness always be technologically possible and reasonable, as a result of the principle of proportionality.[731]

In case that the host provider is obligated to take down or block content due to positive knowledge or obvious unlawfulness, this obligation requires wide-ranging measures. Access of any third party has to be prevented[732] and the host provider has to make sure that no similar infringements occur, e.g. by implementing word filters to the website to prevent that the same information is uploaded again.[733] The German Federal Court of Justice has ruled that 'similar infringements' are not only identical infringements (the same content, provided by the same user or content provider) but also similar content provided by others. Also, the host provider has the obligation to implement the necessary search measures to find and delete similar infringements.[734] This was confirmed by the Court of Justice of the European Union in its recent Facebook-ruling, in which a provider of a social network was required to search and delete not only identically worded, but also synonymous illegal content posted by its users.[735] Thereby further widening the obligations of the host providers to wide-ranging measures.

6.1. Obligations to implement measures for blocking and taking down content

The digital age and its technological progress come with a broad variety of communication options. New possibilities to communicate bare risks and legal challenges, whenever hate crime, copyright violations, fake news or other unlawful content is subject to expression, instead of an objective and constructive discourse. Because pseudonyms or fake profiles accompany anonymity on the internet, especially social media is affected. Recently a court order of the Berlin Regional Court[736] about a potential insult of Renate Künast,

729 Hoeren, Internetrecht, Page 569, recital 1196.
730 BeckOK InfoMedienR/Paal, TMG § 10 recital 26.
731 JurisPK-Internetrecht/Roggenkamp/Stadler, Kapitel 10 recital. 266 et seq.
732 ibid.
733 BGH - I ZR 18/11 in NJW 2013, 784.
734 BGH - I ZR 18/04 in GRUR 2007, 890.
735 ECJ, C-18/18, in: NJW 2019, 3287.
736 District Court Berlin, - 27 AR 17/19; 27 O 433/19.

who is a member of the German Parliament, on Twitter caused sensation. Künast has been referred to on social media as a 'piece of shit' or 'hazardous waste' amongst other things, and her comments regarding a debate about impunity for sex with children have inter alia been dubbed 'perverse', 'sick' and 'abnormal'.[737] Because her statement has been taken out of context she claimed pursuant to Section 14 subsection 3 TMG in conjunction with Section 1 subsection 3 NetzDG to disclose the personal data of those who expressed themselves and potentially insulted her, in order to make civil law claims, for example from Section 823 subsection 2 BGB in conjunction with Sections 185 et seq. StGB, which apply for insults.[738] Surprisingly the court classified the said critical expressions as opinions. Statements of opinion are not punishable according to Sections 185 et seq. StGB, which is why it considered the plaintiff's claim to be non-existent and dismissed it as unfounded.[739] In justifying its ruling the Court said that the statements mentioned above were part of an objective and rational argument.[740] In addition, politicians would have to accept defamatory statements to a greater extent. Later the Berlin Regional Court decided that Künast at least has a right pursuant to Section 14 subsection 3 TMG in conjunction with Section 1 subsection 3 NetzDG regarding wrongly attributed quotes.[741]

These partly contradictory and confusing statements by the Court lead to the question if internet intermediaries are liable for available content on their platforms and whether they are obliged to block or take down illegal content.

6.1.1. General liability for own content

To begin with everybody, including users and intermediaries, can be held responsible for its own content (*principle of personal responsibility*).

According to this the general legal provision is applicable, like in the analogue world. Transporting the European E-Commerce-Directive (Directive 2000/31/EC) into German law Section 7 of the German Telemedia Act clarifies that these rules also apply on service providers within the meaning of Section 2 sentence 1, number 1 TMG. For on-demand audiovisual media services, the service provider is any natural or legal person who effectively controls the selection and design of the content offered. Therefore they are, like their users, accountable for own content.[742]

737 ibid.
738 ibid.
739 ibid.
740 ibid.
741 Redaktion beck-aktuell, becklink 2014911, beck-online.de accessed 4. December 2019.
742 Pille, NJW 2018, 3545.

As a consequence, service providers are obligated to natural restitution, which means according to Section 249 subsection 1, sentence 1 of the German Civil Code they have to re-establish the original state of being. It follows that they have to delete or block content, if they distribute their own insulting content, abusive criticism or fake news or adhere for their own content in any other way. The most important basis of liability is Section 823 subsection 1 BGB in conjunction with Section 1004 Subsection 1, sentence 1 BGB analogue. The provision establishes a liability for any person who interferes with the property or other rights of another (*Störerhaftung*). Furthermore, the disrupter is obligated to refrain from prospective comparable behaviour (Section 1004 subsection 1, sentence 2 BGB analogue). In addition to the obligation deriving from Section 1004 BGB intrusive intermediaries have to delete content, if they can be held accountable by tort law (Sections 823 et seq. BGB).[743] Concerning inaccurate or false factual claims the liability follows Section 824 subsection 1 BGB as more specific regulation.[744] Statements of fact are past or present circumstances that, unlike opinions, are accessible to objective evidence.[745] They are only covered by Article 5 subsection 1, sentence 1 of the German Basic Law if they are basis or connected with an opinion.[746] The defendant must then demonstrate the truth of the factual claim and, if necessary, prove it.[747] The Federal Court of Justice assumes that the first disseminator must also take care of the elimination of factual allegations on other services.[748]

For offensive content Section 823 subsection 2 BGB in conjunction with Sections 185 et seq. of the German Criminal Code can be used to justify deletion obligations. In the context of interpreting the disputed statement the high importance of freedom of expression in a democratic constitutional state must be adequately taken into account (interaction theory) and brought into line with the interests of the person concerned (practical concordance).

Other claims from Section 97 subsection 1, sentence 1 of the Act on Copyright and Related Rights in the event of copyright infringement, Section 14 subsection 5 and Section 15 subsection 4 of the Act on the Protection of Trade Marks and other Signs in protecting trademarks or Section 9 Act Against Unfair Competition regarding unfair business dealings play a rather subordinate role.[749]

743 BGH - VI ZR 340/14; Pille, NJW 2018, 3545.
744 BGH - VI ZR 120/10, in: NJW 2011, 2204.
745 BeckOK Grundgesetz/Schemmer, 42. Ed. 1.12.2019, GG Article 5 recital. 5.
746 ibid., recital. 7.
747 Peifer, NJW 2016, 23 et seq.
748 cf. BGH - VI ZR 340/14, in: NJW 2016, 56.
749 BeckOK InfoMedienR/Paal, 26. Ed. 1.8.2019, TMG § 7 Rn. 5.

However, the question arises to what extent internet intermediaries have to vouch for shared third-party content.

In this respect, liability for third-party statements that the intermediary adapts as its own is unproblematic (espoused third-party content).[750] This is the case if the content responsibility for the contribution is clearly recognisable from the outside.[751] This is made particularly clear from Section 824 BGB.[752]

In summary, it can be said that service providers who provide own or adapted content on the internet (content providers) are unanimously liable according to the relevant standards described above and are responsible for the deletion of the content concerned.

6.1.2. Liability for third-party content

So far, the person concerned had to inform the intermediary about the allegedly illegal content so that the service provider could clarify the facts and carry out a legal evaluation, whereby the author of the potential impairment is given the opportunity to comment if the content is not obviously unlawful or punishable, such as child pornography or sedition.[753] The importance of anonymity, the right to honour of the person concerned and the Freedom of Expression of those who express themselves must be taken into account in the legal evaluation by the intermediary.

Based on these obligations the operator is obliged to delete if he comes to the conclusion that the content is unlawful. The reason for this is the maintenance and spread of the legal impairment by providing the infrastructure as an indirect disruption (interference liability).

This is based on the basic idea of personal responsibility. In order not to impair the functioning of the intermediaries' platform, the Federal Court of Justice expressly differentiates between claims for damages on the one hand and claims for removal or injunctive relief on the other hand. The former only exists if the offense is attributable to the defendant in accordance with the criminal law concept of perpetration and participation as a party to the offense within the meaning of Section 28 subsection 2 StGB. This is the case if he wanted the success of the predicate offence or at least accepted it.[754] The latter, on the other

750 Spindler/Schuster, Elektron. Medien/Hoffmann/Volkmann, 4. Aufl. 2019, TMG § 7 Rn. 14; Peifer, NJW 2016, 23.
751 BGH - VI ZR 123/16, in: NJW 2017, 2029.
752 BGH - VI ZR 269/12, in: NJW 2013, 2348.
753 District Court Würzburg - 11 O 2338/16 UVR, in: MMR 2017, 347.
754 BGH, - I ZR 18/11, in: NJW 2013, 784; Heine/Weißer, Schönke/Schröder, StGB, 29. Aufl. 2014, § 27 Rn. 8; Peifer, NJW 2016, 23, 24.

hand, arises when the defendant is liable as a disruptor, because he wilfully and adequately caused the success without wanting the same.[755] In this way the deletion or elimination is effectively enforced without overburdening the function of the intermediary with the obligation to pay compensation. Elsewhere the Federal Court of Justice seems to differentiate otherwise. In terms of terminology, however, only the intellectual disseminator, i.e. the immediate disruptor referred to above as the participant and the technical disseminator referred to as the indirect disruptor. According to this differentiation, the liability privilege of Section 10 TMG does not apply to providers of social networks who are neither perpetrators nor assistants of the illegal content published on their platform by third parties.[756]

According to Section 7 subsection 2 sentence 2 TMG, there is also an obligation to block without criminal or tortious liability.[757]

This consideration is rooted in the liability privilege of the Telemedia Act.[758] The court also took up ideas on horisontal deletion obligations of the proposals for Article 17 subsection 2 lit. a GDPR (*Right to be Forgotten*). The information about the request for deletion should be used to reverse the distribution chain. This obligation also applies to those responsible according to the Federal Court of Justice outside of the GDPR.[759]

As already indicated the liability of the intermediary for third-party content poses challenges, because the actual disruptor can often not be held responsible directly hence the anonymity shown above.[760] To solve this problem, on the one hand, the obligation to surrender the personal data of the immediate disruptor or your own liability, as well as statutory deletion obligations, come into consideration.

The Berlin Regional Court also decided the first by partially granting the appeal in the Künast case.[761] A right to information is finally regulated in Section 14 subsection 3 TMG and therefore limited to the cases of Section 1 subsection 3 NetzDG. Similarly, the Federal Court of Justice, which derives a basic civil right to information from Section 242 BGB, but rejected with regard to Section 14 subsection 2 TMG and directed the injured party to file a criminal complaint and to inspect the investigation file.[762] According to Section 14 subsection 2 TMG,

755 BGH - I ZR 139/08, in: GRUR 2011, 152.
756 District Court Würzburg - 11 O 2338/16 UVR, in: MMR 2017, 347.
757 BGH - I ZR 304/01, in: MMR 2004, 668.
758 Peifer, AfP 2014, 18, 20.
759 BGH - VI ZR 340/14, in: NJW 2016, 56.
760 Richter, ZD-Aktuell 2017, 05623.
761 Press communique of the District Court Berlin No. 4/2020 – 21 January 2020.
762 BGH - VI ZR 345/13, in: MMR 2014, 704.

the inventory data was only released to law enforcement and security authorities for the purpose of legal prosecution, i.e. permissible for criminal content or for intellectual property violations.[763] A draft amendment to Section 14 subsection 2 TMG provides for the addition of other absolutely protected legal assets in addition to enforcement in the area of intellectual property – also against users.[764] Due to the previous regulation, gaps in regulation only arise where there is no criminal behaviour, especially in the case of unfavourable ratings in online portals. However, these are covered by Section 35 subsection 1 sentence 1 BDSG.[765] In this respect, Section 14 subsection 3 TMG represents a new regulation that should facilitate the enforcement of civil law claims and thus the deletion of illegal content. In line with the liability for interference and personal responsibility, the person responsible for the strengthening should be taken as far as possible.

Service providers who provide third- party information or access to their use (access provider) are privileged in accordance with Sections 8 to 10 TMG, but remain obliged to delete or block illegal content according to Section 7 subsection 2 TMG. According to Section 10 subsection 1 sentence 1 number 1 TMG, damage and criminal liability for unlawful contributions only comes into consideration if the affected content is not deleted immediately after gaining knowledge of the relevant subject or, in the case of tortious liability, from obvious facts that substantiate the unlawful liability (notice and take down principle).[766] Concerning evidently illegal content the characteristic 'immediately' states an obligation to act within 24 hours pursuant to Section 3 subsection 2 number 2 NetzDG.[767] Regarding other unlawful content the intermediary is generally obliged to block or delete the infringement within seven days.[768] The deadline can be exceeded or extended in exceptional cases, if the decision on the illegality of the content depends on the falsehood of a factual claim or on other factual circumstances, depending whether the intermediary has to grant the opportunity to react to the person concerned (cf. Section 3 subsection 3 number 3 lit. a NetzDG) .[769] If he comes to the conclusion that content is not unlawful, the ground will also be removed from later deletion.[770] The rigid deadlines mentioned above exceed Article 14 I E-Commerce-RL. In the case of a design that complies with the guidelines, it therefore remains to be considered in

763 Richter, ZD-Aktuell 2017, 05623.
764 Bundesrat-Drucksache. 315/17.
765 Richter, ZD-Aktuell 2017, 05623.
766 Richter, ZD-Aktuell 2017, 05623.
767 Guggenberger, NJW 2017, 2577, 2578.
768 ibid. 2577, 2579.
769 ibid.
770 Bundestag-Drucksache:. 18/13013, 23; Guggenberger, NJW 2017, 2577, 2579.

individual cases, depending on the obviousness and the severity of the violation.[771]

However, this does not result in a general obligation to monitor, as Section 7 subsection 2 TMG shows as a simple legal implementation of Article 15 RL 2000/31/EG. The operator may be obliged to prevent similar legal violations if it is reasonable for him.[772] This is rejected by non-professional operators, but was last accepted by the Würzbug Regional Court[773] in the case of a selfie of a Syrian refugee with Chancellor Angela Merkel for Facebook.[774]

The Hamburg Higher Regional Court decided otherwise.[775] With regard to the recent case law of the Court of Justice of the European Union, however, the Würzburg District Court must be followed. Specifically, core violations of the law must be prevented in the future.[776]

According to the case law of the Court of Justice of the European Union – contrary to the Federal Court of Justice[777] – the privileged liability also extends to injunctive relief.[778]

The Court of Justice of the European Union decided on a different solution than the above-mentioned extension of liability by the Federal Court of Justice.[779] In the Google Spain case, the Court ruled that the liability and obligations of the initiator of the initial notification should not be extended, as with the Federal Court of Justice. On the contrary the concept of interference (*Störerhaftung*) was extended to the intermediary.[780] The Federal Court of Justice's solution is only useful if the source of the content can be identified.[781] This is particularly problematic because the platform operator must not disclose the anonymity of the person making the statement without its consent.[782]

6.1.3. NetzDG

The legislator has also recognised the difficulties associated with the anonymity of the first person responsible and launched the draft law to improve law enforcement in social networks (NetzDG) on the 5 April 2017. The aim is to

771 Guggenberger, NJW 2017, 2577, 2579.
772 Jandt, in: Roßnagel: BeckRTD-Kommentar, § 10 TMG Rn. 56 ff.; 74 ff.
773 District Court Würzburg, 11 O 2338/16 UVR, in: MMR 2017, 347.
774 OLG Düsseldorf - I-15 U 21/06, in: MMR 2006, 618.
775 OLG Hamburg - 5 W 75/16, in: MMR 2018, 621.
776 Spindler, NJW 2019, 3274.
777 BGH - I ZR 304/01, in: MMR 2004, 668.
778 ECJ -C-70/10, in:, GRUR 2012, 265, 267.
779 BGH - VI ZR 340/14, in: NJW 2016, 56
780 ECJ - C-131/12, in: NJW 2014, 2257.
781 Peifer, NJW 2016, 23.
782 BGH - V ZR 196/11, in: NJW 2012, 2651.

fight hate crime, punishable fake news and other unlawful content in social networks more effectively and to enforce their deletion.[783]

The NetzDG only applies to telemedia providers who operate social networks with the intention of making a profit (Section 1 subsection 1, sentence 1 NetzDG). This refers to platforms on the internet that enable users to exchange, share or make any content available with other users. Professional networks or thematic evaluation portals should explicitly not be covered by the scope of providers in their terms and conditions.

Domestic social networks with less than two million users are also excluded according to Section 1 subsection 2 NetzDG. Users are not just account holders, but all natural or legal persons who use the platform's infrastructure without access to access content and obtain information.[784] So it depends on the number of recipients of the content and not the active users. Also, journalistic editorial offers, e.g. online newspapers with comment function, that are the responsibility of the provider themselves are not scoped (Section 1 subsection 1 sentence 2 NetzDG). This primarily covers large social networks (personal scope).

Illegal contents within the meaning of the law are listed in Section 1 subsection 3 NetzDG, whereby the realisation of the facts is sufficient. There is no need to act guiltily (objective scope).[785]

Section 1 subsection 3 NetzDG concretises the deletion obligations shown above in such a way that obviously illegal content must be blocked or removed within 24 hours after receipt of the complaint. No new deletion obligations are established, but the obligations described above are specified.[786] The deadlines also apply to Section 10 subsection 1 sentence 1 TMG. For copies and reproductions of the infringement, the previous case law in the form of Section 3 subsection 2 number 6 NetzDG has expressly found its way into simple law.

The law also aims to create transparency through a reporting obligation, in which the platform operator discloses its handling of complaints by those affected on a quarterly basis so that the criteria on the basis which illegal content can be assessed (see above) can be identified (Section 2 subsection 1 NetzDG).

If the operators do not comply with the obligations outlined, they may face fines of up to EUR 5 million in accordance with Section 4 subsection 1 NetzDG.

783 Bundesrat-Drucksache 315/17.
784 Bundesrat-Drucksache 315/17, pp. 1, 15.
785 Bundesrat-Drucksache 135/17, page 1, 15.
786 Bundesrat-Drucksache 135/17, page 18.

In connection with these obligations, censorship by private providers is often spoken of, although the term is used more colloquially than the pre-censorship covered by Article 5 subsection 1 sentence 3 GG. From a legal point of view, deletion by private individuals is not censorship. As an act of public authority, the law nonetheless constitutes an interference with the fundamental right to Freedom of Expression, which must be constitutionally justified. It has to be measured against the barrier reservation of Article 5 subsection 2 GG. Since the NetzDG is not directed against a specific opinion, it is general law in the sense of the qualified legal reservation. In particular, this must be proportionate.

The impending fines could persuade internet intermediaries to prematurely remove contributions in order to avoid their own liability. This could also affect content that is not covered by the catalogue of Section 1 subsection 3 NetzDG at all.

In addition, the evaluation of behaviour patterns or content as unlawful is carried out by private persons, although this is originally the official responsibility of the state, in particular courts (Article 20 subsection 3 GG). Considering this as a violation of the constitution, the NetzDG can therefore be seen as disproportionate interference with freedom of expression.[787] A solution could be to limit the sanctions to the failure to establish a complaint management system.[788]

In any case, the formal unconstitutionality of the law is assumed in part, because of violating competences to Article 70 GG.[789]

In the case of the Chancellor selfie, the Würzburg District Court, considers the deletion obligation as limited to Germany, despite being available internationally, since there is no international responsibility following Section 35 of the Code of Civil Procedure (Zivilprozessordnung – ZPO). The decision by a German court to delete in another state constitutes an unjustified interference in its powers. A violation of German law does not justify a court order in other countries.[790] In this respect, the possibility of so-called geo--blocking should be used. Illegal content therefore remains available internationally.

The Federal Court of Justice nonetheless considers that German Courts have jurisdiction over international injunctive relief under certain conditions. Responsibility is therefore always given if the contested content has an evident

787 Richter, ZD-Aktuell 2017, 05623.
788 Richter, ZD-Aktuell 2017, 05623.
789 BeckOK InfoMedienR/Hoven/Gersdorf, 26. Ed. 1.5.2019, NetzDG § 1 Rn. 5; Schiff, MMR 2018, 366.
790 District Court Würzburg, 11 O 2338/16 UVR, in: MMR 2017, 347, 349 f.

domestic nexus. Following the Court's ruling this is the case if an acknowledgment of the violation of personality is more likely in Germany, than it would be if the content were only available online. Furthermore, the impairment would also occur in Germany.[791]

With regard to Article 18 ECRL, the Court of Justice of the European Union relies on the fact that it does not provide for any territorial restriction.[792] Nothing else can therefore apply to the TMG, which serves to implement the directive.

The Court of Justice of the European Union does not make any general surveillance obligations either.[793] However, specific core content could be identified by automatic filters, provided the wording is comparable.[794] It is more problematic to filter meaningful expressions with different wording.

6.2. Safeguards ensuring the expression of freedom online.

The procedure of taking down and blocking content by internet intermediaries under the regulations of the NetzDG is supervised by the Federal Office for Justice (*Bundesamt für Justiz*), according to Section 3 Subsection 5 and Section 4 Subsection 4 NetzDG. This procedure has to be documented by the provider (Section 3 Subsection 3 NetzDG) and the involved parties have to be notified immediately, including information about the reasons of the decision (Section 4 Subsection 1 No. 2 NetzDG).[795] This supervision can also be transferred to an instance of self-regulation jointly funded by providers of social networks under the conditions set out in Section 3 Subsection 5 and 6 NetzDG,[796] but no use has yet been made of this possibility. Intent and purpose of these obligations is to make decisions which are restricting the freedom of expression online transparent and to provide a general overview how often and under which circumstance content is taken down by private companies.[797] Although intend of the legislator was especially to secure that the social network are blocking unlawful content, to fight hate speech online,[798] the obligations to inform and give reasons and to document the procedure are in return also serving as a control opportunity if there is any over-blocking unduly restricting the freedom of expression online. [799]

791 BGH - VI ZR 23/09, in: NJW 2010, 1752.
792 ECJ - C-544/15, in: NJW 2017, 3287.
793 Spindler, NJW 2019, 3274, 3275.
794 Spindler, NJW 2019, 3274, 3275.
795 Nomos-BR/Liesching NetzDG/Liesching, NetzDG § 3 recital 18 et seq.
796 ibid. recital 23.
797 Bundestag-Drucksache 18/12356 page 18 et seq.
798 ibid.
799 Löber/Roßnagel MMR 2019, 71.

The Federal Office for Justice is not only supervising the process but is also authorised to fine social networks when they are violating the regulations of the NetzDG, however it shall not do this on its own, pursuant to Section 4 Subsection 5 NetzDG. The conduct of the social network provider and whether or not the content that has not been blocked was unlawful, shall be controlled in advance by a court before a fine can be imposed.[800] Thereby ensuring that the decision which statements are covered by the Freedom of Expression and which are not is made by a court and the principle of separation of power is not undermined.[801]

For the individual user there is no specific legal remedy provided in the NetzDG. If content of him is blocked, he is limited to claims that may exist in the general terms and conditions of the social network. Otherwise he is of course able to assert claims after the general laws against the provider to restore his content.[802] This can also be achieved by an injunction pursuant to Sections 935 et seq. Code of Civil Procedure.[803]

As far as the question whether or not the NetzDG is constitutionality is concerned, there is the possibility for judges confronted with applying the regulations of the NetzDG to raise a concrete judicial review (*konkrete Normenkontrolle*) at the Federal Constitutional Court pursuant to Article 100 Subsection 1 of the Basic Law.[804] Individuals confronted with decisions restricting their right to freedom of expression – not only on basis of the NetzDG but by any administrative or judicial decision - are able to lodge a constitutional complaint (after exhausting all other legal remedies), pursuant to Article 93 Subsection 1 No. 4a Basic Law[805] or even an individual petition based on Article 34 ECHR claiming the infringement of Article 10 ECHR.

800 Spindler/Schmitz/Liesching, NetzDG § 4 recital 32 et. seq.
801 Bundestag-Drucksache 18/12356 page 26 et seq.
802 Schiff, MMR 2018, 366.
803 Koreng, GRUR-Prax 2017, 203.
804 Liesching, MMR 2018, 26.
805 ibid.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1. Future development of the legislation regarding online content blocking and take-down

Following the developments in the Network Enforcement Act and its drafts, it can be assumed that the obligations of private operators will increase. In addition, self-regulation of the private sector is expected to expand. Here the state will be served by reports from private providers. In addition, the State will impose information obligations on private operators, under which the State will receive critical information on specific users. It remains to be seen how the case develops around the prohibition of associations and the deactivation of their websites. Depending on this, specific legislation or jurisdiction may develop in this regard.

7.2. Future development of the liability of internet intermediaries

Regarding the liability of internet intermediaries, similar predictions can be made. Liability developed in a way that platform operators can in principle also be held responsible for third-party content, but at least are obligated to delete unlawful content. On that basis it can be assumed that internet intermediaries are going to be more involved in law enforcement on the internet.

Because the internet is a fast developing medium, legislative changes can only follow one or two steps behind. That makes it hard to predict which changes and which new regulations have to be enacted to ensure the liability of internet intermediaries in the future. With new technology possibilities - especially due to the enhancement of artificial intelligence - it is questionable if the 'notice and take down'-procedure will still be able to provide a satisfying solution or if higher requirements have to be set. Also, it has to be observed if the distinction between content, access and host providers in the Subsection 7 et seq. TMG is future proof or if an even more differentiated solution has to be found. Due to the unpredictability of the development of the internet such changes and adjustments should not be made rash but on the other hand it would also be irresponsible of the legislators to not watch the changes and find reasonable solutions in due time.

7.3. Future development of the right to be forgotten

As the European Union has regulated the right to be forgotten in the GDPR, there is only little room for the German legislators for any further activity in this field. This is a result of the full harmonisation which accompanies every directive by the European Union pursuant to Article 288 Subsection 2 TFEU. Even Though 'gold plating' regulations by the German legislator could be conceivable, it does not seem very likely as he used possibilities granted by opening clauses in the GDPR to weaken the rights granted there.[806]

Nonetheless there is the possibility to work on the concretisation of the GDPR in the German BDSG if there is a corresponding opening clause. Especially regarding Section 35 BDSG a revision would be appropriate due to the facts stated above, to ensure the conformity with the European legislation. However, the BDSG was just changed in November 2019,[807] without showing an interest to the criticism voice concerning Section 35 BDSG and any further changes are not to be predicted for the next period, nor discussed.

Another possibility to strengthen the right to be forgotten would be to establish a specific basic right to privacy in the German Basic Law as it is in Article 8 ECHR, but due to the high demands needed to change the Basic Law (according to Article 79 Subsection 1 and 2 GG) and the current majorities in the German parliament such an amendment of the constitution does not seem likely.

Even though the introduction of an explicit right to privacy is unlikely, the Federal Constitutional Court has strengthened the right to be forgotten in its recent rulings,[808] ensuring that the explicit right to privacy granted in Article 8 ECHR will be considered in further judgments, as long as Article 17 GDPR or any other law fully determined by European Union Law is concerned.

806 Paal/Pauly/Paal, BDSG § 35 recital 2.
807 BGBl. I S. 1626.
808 BVerfG - 1 BvR 16/13, 1 BvR 276/17.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

According to prevailing opinion in the legal literature, such an adequate balance has not (yet) been found. While the intention of the Network Enforcement Act is generally seen as positive, there is a deficiency in its implementation.[809]

Particular criticism is levelled at the fundamentally repressive orientation of the Network Enforcement Act, which can easily lead to over-blocking. Insofar, amendments are suggested which are intended to actively protect freedom of expression (Put-back procedure).[810]

There are also concerns that Article 5 GG could be violated by the Network Enforcement Act and that it is therefore unconstitutional.[811] Furthermore, there are concerns about admissibility under European law, because the flexible deadline of the relevant e-commerce Directive[812] is replaced by rigid deadlines in national law.[813] In summary, it must be stated that the German legislator still has to make improvements at this point in order to achieve a balance between allowing freedom of expression online and protecting against hate speech in the online environment. Consideration should also be given to whether there is not rather a lack of enforcement and whether the regular civil and criminal laws are not already sufficient, i.e. simply need to be applied effectively.

The following amendments are proposed:[814]

- Simplification of the reporting channel, in particular the possibility of reporting in direct connection with the content and not exclusively via a form that can be accessed separately.
- Introduction of an obligation to restore content that has been unlawfully removed and to report such cases.
- Report on content deleted according to internal rules of the platform.
- Mandatory forwarding of criminally relevant content to the prosecution authorities. (This amendment was made recently.)[815]

809 Löber/Roßnagel, MMR 2019, 71.
810 Peukert, MMR 2018, 572.
811 Liesching, MMR 2018, 26; Schiff, MMR 2018, 366.
812 Article 14 I lit. b RL 2000/31/EG.
813 Paragraph 3 Section 2 Numbers 2 and 3 Network Enforcement Act; Koreng, GRUR-Prax 2017, 203; Liesching, MMR 2018, 26.
814 Löber/Roßnagel, MMR 2019, 71.
815 Bundestag-Drucksache 19/17741, page 41.

In addition, platforms should be self-regulated by an independent body - comparable to self-regulation in the entertainment software industry - which is provided for by law but has not yet been implemented in practice. On 13 January 2020 the '*Freiwillige Selbstkontrolle Multimedia-Anbieter e.V.*' (FSM)[816] was officially recognised[817] as an institution of regulated self-regulation. The institution will begin its work in the next few weeks. Members of the FSM include Facebook and Snapchat, two of the largest social media platforms in Germany.[818]

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

The right to freedom of expression is guaranteed by Article 5 Subsection 1 GG. This applies for the analogue world and activities on the internet. As a basic right the freedom of speech is granted with a high level of protection, as according to Article 79 Subsection 2 GG a two-thirds majority indispensable to constitutional amendments. Its interpretation by the German Constitutional Court is binding. Furthermore, the right deriving from Article 5 Section 1 Sentence 1 GG is a fundamental right in a democracy, as Freedom of Speech is essential to political discourse and formation of opinion.

Due to conflicting rights the Right to Freedom of Expression cannot be guaranteed without limits. On the internet the most common actions that restrict the Freedom of Expression are filters and blockings. According to Article 5 Subsection 2 GG these restrictions can only occur on the basis of general laws, which are the biggest weak point for criticism as they regulate the extent of the Freedom of Expression on the internet.

Having said this, from a historic point of view the fundamental function of basic rights is protection of the citizens against government interferences, which means that basic rights are mandatory to public authorities. But interference on the internet is often caused by private individuals. Therefore, it is inalienable to stipulate private actions as detailed as possible (*Wesentlichkeitstheorie*), whenever they act like authorities or fulfill public tasks on behalf of a public authority. It even seems questionable whether individuals should be allowed to interfere in one of the most sensible areas of the constitution. The necessity of strict and

816 FSM, <https://www.fsm.de/de/netzdg>, accessed 28 February 2020.
817 BfJ, <https://www.bundesjustizamt.de/DE/Presse/Archiv/2020/20200123.html> accessed 2. February 2020.
818 FSM, <https://www.fsm.de/de/verein#A1_3>, accessed 28 February 2020.

clear guidelines was seen by individuals too, as they have an interest to compile to these rules and avoid liabilities. Recently, Mark Zuckerberg, founder and CEO of Facebook, criticised the applicable rules as imprecise.[819] They lead to legal insecurities and possibly even unwanted violations of these regulations for fear of potential liabilities. Due to the monopoly position of internet intermediaries the state has the obligation to protect the freedom of speech, which underlines the importance of clear stipulation. Therefore, Freedom of Expression must be maintained as far as possible, whilst taking third-party rights into consideration adequately (*Praktische Konkordanz*). On the one hand the importance of Freedom of Expression to a democracy and on the other hand the number of interferences or people affected or concerned by unlawful activities on the internet must be taken into account.

Since all interests must be taken into account in the weighing of individual cases, Freedom of Expression is in any case adequately protected in theory if legal violations on the Internet are punished by state authorities. In practice, the high number of individual cases is a seemingly impossible task for the authorities. Because of this the approach to obligate intermediaries to report violations to public authorities is a step in the right direction.

However, the NetzDG as a barrier to the Freedom of Speech, might conflict with the Basic Law. This is not acceptable. On the other hand, there are definitely some positive points to mention about the current legislation regarding the right to freedom of expression online. Some of the relevant provisions provide room for an appropriate weighting between colliding interests. This creates space for a fair decision in the particular case and to guarantee the Freedom of Expression to the maximal extent.

In conclusion the Right to Freedom of Speech might never be granted to its fullest extent, because of rapid technological development, legal adjustments, human mistakes or mechanical errors by blocking or deleting content, which can never be ruled out completely, but is protected in a proper way. Due to the high demand caused by the high number of individual cases, increasing personnel of public authorities would be a practicable approach.

819 Facebook löscht täglich 1 Million Fake-Konten, <https://www.faz.net/aktuell/wirtschaft/facebook-loescht-taeglich-1-million-fake-konten-16635950.html?fbclid=IwAR0RP8jVr_94K4r2LeyCUtxqF7ENvn_3P-ydlPtsrt1ryleAB_bnlsBMTro&utm_campaign=GEPC%253Ds6&utm_content=bufferecd02&utm_medium=social&utm_source=facebook.com> accessed 16 February 2020.

10. How do you rank the access to freedom of expression online in your country?

We would rank the access to freedom of expression online in Germany with the mark of 4 (with 5 being the best possible mark).

As explained above, freedom of expression is in principle a good that is particularly protected by the German constitution. Nonetheless there are issues at hand that need to be regulated by the legislator. While the problem of general access to internet as foundation for the possibility to express an opinion online has successfully been solved, (46% of all households had Internet access in 2002, this figure has been growing steadily, reaching 94% in 2018),[820] the current developments like the NetzDG have to been watched critically and changed if needed. Also, the self-regulation by private operators could proof dangerous and could either to decline of freedom of expression online or to an overregulation, unlawfully harming other constitutional values and thus needs to be evaluated.

In general the protection of Freedom of Expression online is not flawless in Germany, especially because a perfect balance between freedom of expression and the protection of third party rights has not yet been found, but we are far from a situation that would endanger the most important purpose which the Federal Constitutional Court adjudged to Freedom of Expression: the purpose of constituting democracy.[821]

11. How do you overall assess the legal situation in your country regarding internet censorship?

Recently, German law mainly focuses on internet content that is published in social media. There are positive developments in this regard, but the current legal situation needs to be refined. In particular that there is no legal regulation on grievance redressal mechanisms is negative. Self-regulation by private operators has many advantages, but also disadvantages. It is possible that the measures taken by private operators are not sufficient. In this regard, it may be useful to consider further sanctions against private operators that go beyond simple fines. The fact that the Federal Ministry of the Interior has deactivated a journalistic website due to the law on associations is a very critical matter from the point of

820 Statista, <https://de.statista.com/statistik/daten/studie/153257/umfrage/haushalte-mit-internetzugang-in-deutschland-seit-2002/>, accessed 16 February 2020.

821 BVerfG, 1 BvR 400/51; 1 BvR 586/62, 610/63, 512/64.

view of freedom of expression.[822] There is a need for clear case law and, where necessary, legislation. This is because the monitoring of internet content is basically a matter for the federal states in accordance with Section 59 Subsection 2 of the Broadcast State2Treaty. In addition, the Broadcast State Treaty primarily provides the blocking of illegal content in the case of violations of the law. However, the Federal Ministry of the Interior has deactivated the entire website. These discrepancies must be clarified. But the fact that in Germany the legal material about internet providers has been unified in the Tele Media Act and a separate legal basis has been created for the social media is very positive. The fact that the federal states continue to deal with the matter and have signed state treaties is also very positive. However, recent developments and discussions show that both society and politics have recognised this field and its problems. The most important thing is that the state does not intervene disproportionately in this matter and does not create the impression of arbitrarily blocking content. For this reason, the legal starting position in Germany with regard to internet censorship is generally good.

[822] Announcement of an association ban against „linksunten.indymedia" from 14 August 2017 by the Federal Ministry of the Interior, BAnz AT 25 August 2017 B1, <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2017/verbotsverfuegung-linksunten.pdf?__blob=publicationFile&v=1>.

Conclusion

As lined out in this report, there are two main questions when reviewing Internet Censorship in Germany. First if appropriate and contemporary rules are applied and second, if the fine line between protecting third-party rights and violating the Freedom of Expression online is not crossed. Regarding the application of appropriate and contemporary rules it has become obvious, that due to the fast pace of development of the internet the legislator is always only able to react and not able to anticipate any future developments. The approach of self-regulation by the internet intermediaries could be an approach to get closer to the pulse of development, but of course must be further evaluated, especially as protection fundamental rights should not be 'outsourced' to private operators. Furthermore, on the one hand the struggle with the competence structure between the European Union and the Federal Republic of Germany and between the federal government of Germany and the different federal states can lead to some legal uncertainty or delay in finding contemporary rules, but on the other hand this also ensures 'checks and balances' when finding appropriate rules. As far as the relationship between the protection of third-party rights and the protection of freedom online is concerned, Germany can be considered on a good path, and there is no real danger, that freedom of expression online could be extensively censored. But of course, there is scepticism and criticism regarding legislation limiting freedom of expression online, which is good and shows that there is awareness in the society regarding this topic and the 'public watch dogs' are functioning. Nonetheless the further development has of course to be watched, the impact has to be evaluated and the legislator is – especially in light of the importance of Freedom of Expression for a functional democracy and the encouraging jurisdiction of the Federal Constitutional Court – obliged to adjust the rules if necessary and ensure that the Freedom of Expression online is also guaranteed in the future.

Table of legislation

Bundesdatenschutzgesetz alte Fassung (BDSG a. F.) - Federal Data Protection Act (old version)

Provision in German language	**Corresponding translation in English**
§ 20 - Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht (1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten. (2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. (3) An die Stelle einer Löschung tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. (...)	§ 20 - Correction, deletion and blocking of data; Right to object (1) Personal data must be corrected if it is incorrect. If it is determined that personal data that is neither automatically processed nor stored in non-automated files is incorrect, or if the data subject disputes its accuracy, this must be recorded in an appropriate manner. (2) Personal data that is processed automatically or stored in non-automated files must be deleted if their storage is prohibited or their knowledge is no longer required for the responsible body to fulfill the tasks within their area of responsibility. (3) Instead of a deletion, data has to been blocked, if legal, statutory or contractual retention periods prevent deletion, There is reason to believe that deletion would affect the data subject's legitimate interests, or deletion is not possible due to the special type of storage or is only possible with disproportionate effort. (...)
§ 35 - Berichtigung, Löschung und Sperrung von Daten (1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.	§ 35 - correction, deletion and blocking of data (1) Personal data must be corrected if it is incorrect. Estimated data must be clearly identified as such.

Geschätzte Daten sind als solche deutlich zu kennzeichnen. (2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn ihre Speicherung unzulässig ist es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungs-widrigkeiten handelt und ihre Richtigkeit von der verant-wortlichen Stelle nicht bewiesen werden kann, sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist. Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt. (...)	(2) Personal data can be deleted at any time except in the cases of paragraph 3 No. 1 and 2. Personal data must be deleted if their storage is not permitted it is data about racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, health, sex life, criminal acts or administrative offenses and their correctness cannot be proven by the responsible body, they are processed for own purposes as soon as their knowledge is no longer necessary for the fulfillment of the purpose of the storage, or they are processed commercially for the purpose of transmission and an examination is carried out at the end of the fourth calendar year, insofar as it concerns data on completed matters and the data subject does not object to the deletion, at the end of the third calendar year, beginning with the calendar year following the first storage, shows that long-term storage is not necessary. Personal data that is stored on the basis of § 28a (2) sentence 1 or § 29 (1) sentence 1 No. 3 must also be deleted after termination of the contract if the person concerned so requests. (...)

Telemediengesetz (TMG) - Telemedia Act

Provision in German language	**Corresponding translation in English**
§ 1 - Anwendungsbereich (1) Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über	Section 1 - Scope (1) This Act shall apply to all electronic information and communication services unless they are telecommunications services according to Section 3 No. 24 of the Telecommunications Act, which consist entirely in the transmission of signals via

Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.	telecommunications networks, telecommunications-supported services according to Section 3 No. 25 of the Telecommunications Act or broadcasting according to Section 2 of the State Broadcasting Treaty (telemedia). This Act applies to all providers, including public authorities, independently of whether a charge is levied for.
§ 7 - Allgemeine Grundsätze (1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich. (2) Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. (3) Verpflichtungen zur Entfernung von Informationen oder zur Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen aufgrund von gerichtlichen oder behördlichen Anordnungen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Das Fernmelde-geheimnis nach § 88 des Telekommunikationsgesetzes ist zu wahren. (4) Wurde ein Telemediendienst von einem Nutzer in Anspruch genommen, um das Recht am geistigen Eigentum eines anderen zu verletzen und besteht für den Inhaber dieses Rechts keine andere Möglichkeit, der Verletzung seines Rechts abzuhelfen, so kann der Inhaber des Rechts von dem betroffenen Diensteanbieter nach § 8 Absatz 3 die Sperrung der Nutzung von Informationen verlangen, um die Wiederholung der Rechtsverletzung zu verhindern. Die Sperrung muss zumutbar und verhältnismäßig sein. Ein Anspruch gegen den Diensteanbieter auf Erstattung der vor- und außergerichtlichen Kosten für die Geltendmachung und Durchsetzung des	§ 7 - General principles (1) Service Provider are responsible for own information, which they hold available for usage, under the general laws. (2) Service Provider within the meaning of the §§ 8 to 10 are not obligated to supervise the information transmitted or saved by them or to search for circumstances that indicate illegal activity. (3) Obligations to remove information or to block the use of information in accordance with the general laws due to court or official orders remain unaffected even in the case of the service provider's non-responsibility in accordance with Sections 8 to 10. The secrecy of telecommunications according to Section 88 of the Telecommunications Act must be maintained. (4) If a telemedia service has been used by a user in order to infringe the intellectual property right of another user, and if there is no other possibility for the holder of this right to remedy the infringement of his right, the holder of the right may demand that the service provider concerned block the use of information in accordance with Section 8 Subsection 3 in order to prevent the repetition of the infringement. The blocking must be reasonable and proportionate. A claim against the service provider for reimbursement of the pre- and out-of-court costs for asserting and enforcing the claim pursuant to sentence 1 does not exist, except in the cases of Section 8 Subsection 1 Sentence 3.

Anspruchs nach Satz 1 besteht außer in den Fällen des § 8 Absatz 1 Satz 3 nicht.	
§ 8 - Durchleitung von Informationen (1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie die Übermittlung nicht veranlasst, den Adressaten der übermittelten Informationen nicht ausgewählt und die übermittelten Informationen nicht ausgewählt oder verändert haben. Sofern diese Diensteanbieter nicht verantwortlich sind, können sie insbesondere nicht wegen einer rechtswidrigen Handlung eines Nutzers auf Schadensersatz oder Beseitigung oder Unterlassung einer Rechtsverletzung in Anspruch genommen werden; dasselbe gilt hinsichtlich aller Kosten für die Geltendmachung und Durchsetzung dieser Ansprüche. Die Sätze 1 und 2 finden keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen. (2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist. (...)	§ 8 - Transmitting information (1) Service providers are not responsible for external information that they transmit in a communication network or to which they provide access, provided that they, do not initiate the transmission, did not select the addressee of the transmitted information and have not selected or changed the transmitted information. If these service providers are not responsible, they cannot be held liable in particular not because of an illegal act by a user for compensation or elimination or omission of an infringement; the same applies regarding to all costs for the assertion and enforcement of these claims. Sentences 1 and 2 do not apply if the service provider intentionally works with a user of his service to commit unlawful acts. (2) The transmission of information in accordance with section 1 and the provision of access to it also includes the automatic short-term intermediate storage of this information, as much as this only takes place for the transmission to be carried out in the communication network and the information is no longer stored than is normally required for the transmission. (...)
§ 9 - Zwischenspeicherung zur beschleunigten Übermittlung von Informationen Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie	§ 9 - Intermediate storage for accelerated transmission of information Service providers are not responsible for automatic, temporary restricted intermediate storage, which serves the sole purpose of making the transmission of third-party information to other users at their request more efficient, provided that they do not change the information,

die Informationen nicht verändern, die Bedingungen für den Zugang zu den Informationen beachten, die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten, die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erhalten haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat. § 8 Abs. 1 Satz 2 gilt entsprechend.	observe the conditions for access to the information, comply with the rules for updating the information set out in widely recognized and used industry standards, do not affect the permitted use of technology to collect data on the use of the information set out in widely recognised and used industry standards, and act immediately in order to remove or to block access to information stored within the meaning of this regulation as soon as they have become aware that the information was removed from the network at the original point of transmission or access to it was blocked or a court or an administrative authority has ordered removal or blocking. § 8 (1) sentence 2 is applied accordingly.
§ 10 - Speicherung von Informationen Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatz-ansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben. Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.	§ 10 - Storage of information Service providers are not responsible for external information that they store for a user, provided that they have no knowledge of the illegal act or the information and, in the event of damage claims, they are also not aware of any facts or circumstances from which the illegal act or the information becomes obvious, or they acted immediately to remove the information or to block access to it as soon as they became aware of it. Sentence 1 does not apply if the user is subordinate to the service provider or is supervised by him.

Vereinsgesetz (VereinsG) - Association Act

Provision in German language	**Corresponding translation in English**
§ 2 - Begriff des Vereins (1) Verein im Sinne dieses Gesetzes ist ohne Rücksicht auf die Rechtsform jede Vereinigung, zu der sich eine Mehrheit natürlicher oder juristischer Personen für längere Zeit zu einem gemeinsamen Zweck freiwillig zusammengeschlossen und einer organisierten Willensbildung unterworfen hat. (2) Vereine im Sinne dieses Gesetzes sind nicht 1. politische Parteien im Sinne des Artikels 21 des Grundgesetzes, 2. Fraktionen des Deutschen Bundestages und der Parlamente der Länder.	Section 2 - Definition of Association (1) For the purposes of this Act, an association is any association, irrespective of its legal form, in which a majority of natural or legal persons have voluntarily joined together for a longer period of time for a common purpose and have submitted to an organised decision-making process. (2) Associations in the sense of this law are not 1. political parties within the meaning of Article 21 of the Basic Law, 2. Factions of the German Parliament and the parliaments of the Federal States.
§ 3 – Verbot (1) Ein Verein darf erst dann als verboten (Artikel 9 Abs. 2 des Grundgesetzes) behandelt werden, wenn durch Verfügung der Verbotsbehörde festgestellt ist, daß seine Zwecke oder seine Tätigkeit den Strafgesetzen zuwiderlaufen oder daß er sich gegen die verfassungsmäßige Ordnung oder den Gedanken der Völkerverständigung richtet; in der Verfügung ist die Auflösung des Vereins anzuordnen (Verbot). Mit dem Verbot ist in der Regel die Beschlagnahme und die Einziehung 1. des Vereinsvermögens, 2. von Forderungen Dritter, soweit die Einziehung in § 12 Abs. 1 vorgesehen ist, und 3. von Sachen Dritter, soweit der Berechtigte durch die Überlassung der Sachen an den Verein dessen verfassungswidrige Bestrebungen vorsätzlich gefördert hat oder die Sachen zur Förderung dieser Bestrebungen bestimmt sind, zu verbinden.	Section 3 - Prohibition (1) An association may only be treated as prohibited (Article 9 Subsection 2 of the Basic Law) if it is established by order of the prohibition authority that its purposes or activities are contrary to criminal law or that it is directed against the constitutional order or the idea of international understanding; the order must order the dissolution of the association (prohibition). As a rule, the prohibition shall include the seizure and confiscation 1. of the assets of the association, 2. claims of third parties, insofar as collection is provided for in Section 12 Subsection, and 3. of third party property, insofar as the beneficiary has intentionally promoted the unconstitutional efforts of the association by handing over the property to the association or the property is intended to promote these efforts.

Bibliography

English titles

Digital resources

Oliver Jouanjan, Freedom of Expression in the Federal Republic of Germany, (Indiana Law Journal: Vol. 84, 2009), 867 – 883 <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1126&context=ilj> accessed 5 February 2020

https://www.coe.int/en/web/freedom-expression/internet-intermediaries, accessed 9 February 2020

Case law

ECJ, Glawischnig v Piesczek [2019], C-18/18, published in: NJW 2019, 3287

ECJ, Commission v Italian Republic. - Agricultural producer groups. [1983], C-272/83

ECJ, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014], C-131/12 published in: NJW 2014, 2257

ECJ, Fahimian v Federal Republic of Germany [2016], C-544/15

ECJ, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] C-70/10, published in: GRUR 2012, 265

ECHR, Cengiz and others v Turkey [2015] 48226/10 and 14027/11

ECHR, Yildirim v Turkey [2012], 3111/10

German titles

Legislation

Drucksache des deutschen Bundestages 18/11325 vom 24.02.2017: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

Drucksache des deutschen Bundestages 18/12356 vom 16.05.2017: Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken

Drucksache des deutschen Bundesrates 315/17 vom 21.04.2017: Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)

Drucksache des deutschen Bundestages 19/17741 vom 10.03.2020: Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität

Federal Law Gazette, BGBl. I S. 1626

Books

Wendt, von Münch/Kunig, GG (6th edn, C.H.BECK 2012)

Von der Decken, Schmidt-Bleibtreu/Hofmann/Hennecke, GG (14th edn, Carl Heymanns 2017)

Di Fabio, Maunz/Dürig, GG (88th edn, C.H.BECK, 2019)

Peuker, Sydow (Hrsg.), Bundesdatenschutzgesetz – Handkommentar (1st edn, Nomos, 2019)

Paal, Paal/Pauly Bundesdatenschutzgesetz (2nd edn, C.H.BECK, 2018)

Herbst, Kühling/Buchner, Bundesdatenschutzgesetz (2nd edn, C.H.BECK, 2018)

Pieroth/Jarass, Grundgesetz (15th edn, C.H.BECK, 2018)

Dreier, Grundgesetz (3rd edn., C.H.BECK, 2013)

Hoeren, Internetrecht – Ein Grundriss (3rd edn., De Gruyter, 2017)

Hoffmann/Volkmann, Spindler/Schuster, Recht der elektronischen Medien (4th edn., C.H.BECK, 2019)

Roggenkamp/Stadler, Heckmann, Praxiskommentar-Internetrecht (6th edn., Juris, 2019)

Spindler/Schmitz/Liesching, Telemediengesetz mit Netzwerkdurchsetzungsgesetz (NetzDG) (2nd edn., C.H.BECK, 2018)

Epping/Hillgruber, Grundgesetz (42nd edn., C.H.Beck, 2019)

Gersdorf/Paal, Informations- und Medienrecht (26th edn., 2019)

Schönke/Schröder, Strafgesetzbuch, (29th edn., 2014).

Roßagel, Kommentar zum Recht der Telemediendienste, (2013)

Schoch, Informationsfreiheitsgesetz (2nd edn., 2016)

Periodicals

Roßnagel, Gesetzgebung im Rahmen der Datenschutz-Grundverordnung, in DuD 2017, 27

Helfrich, DSAnpUG-EU: Ist der sperrige Name hier schon Programm?, in ZD 2017, 97

Nolte, Zum Recht auf Vergessen im Internet, in ZRP 2011, 236

Hoffmann, Mittelbare Verantwortlichkeit im Internet, in Jus 2017, 713

Löber/Roßnagel, Das Netzwerkdurchsetzungsgesetz in der Umsetzung, in MMR 2019, 71

Schiff, Meinungsfreiheit in mediatisierten digitalen Räumen, in MMR 2018, 366

Koreng, Entwurf eines Netzwerkdurchsetzungsgesetzes: Neue Wege im Kampf gegen „Hate Speech"?, in GRUR-Prax 2017, 203

Liesching, Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG, in MMR 2018, 26

Kühling, Das „Recht auf Vergessenwerden" vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem, in NJW 2020, 275 ff

Götting, Vom Right of Privacy zum Right of Publicity

Die Anerkennung eines Immaterialgüterrechts an der eigenen Persönlichkeit im amerikanischen Recht in GRUR Int. 1995, 656 ff

Pille, Der Grundsatz der Eigenverantwortlichkeit im Internet, in NJW 2018, 3545 ff

Peifer, Beseitigungsansprüche im digitalen Äußerungsrecht - Ausweitung der Pflichten des Erstverbreiters, in NJW 2016, 23 ff

Peifer, Konvergenz in der Störer- und Verbreiterhaftung - Vom Störer zum Verbreiter?, in AfP 2014, 18 ff

Richter, Das NetzDG – Wunderwaffe gegen „Hate Speech" und „Fake News" oder ein neues Zensurmittel?, in ZD-Aktuell 2017, 05623

Spindler, Weltweite Löschungspflichten bei Persönlichkeitsverletzungen im Internet, in NJW 2019, 3274 ff

Schiff, Meinungsfreiheit in mediatisierten digitalen Räumen, in MMR 2018, 366 ff

Guggenberger, Das Netzwerkdurchsetzungsgesetz in der Anwendung, NJW 2017, 2577

Voßkuhle, Kaiser, Grundwissen - Öffentliches Recht: Funktionen der Grundrechte, JuS 2011, 411

Hühner, Anmerkung zu BGH, Urteil vom 12.07.2012 - I ZR 18/11, GRUR 2013, 373-375

Digital resources

Federal Ministry of the Interior, Building and Community, 'Informationsfreiheitsgesetz' <https://www.bmi.bund.de/DE/themen/moderne-verwaltung/open-government/informationsfreiheitsgesetz/informationsfreiheitsgesetz-node.html> accessed 7 February 2020

Schemmer/Lang, BeckOK Grundgesetz (42th edn, C.H.BECK, 2019)

Worms, Brink/Wolff, BeckOK Datenschutzrecht (30th edn. C.H.BECK, 2019)

Spingler, Gsell et al. BeckOGK, (C.H.BECK, 2020)

Paal/Gersdorf, BeckOK Informations- und Medienrecht (26th edn., C.H.BECK, 2019)

Liesching, Nomos-Bundesrecht – Netzwerkdurchsetzungsgesetz (1st online edn., C.H.BECK, 2018)

The Broadcast State Treaty in the version of his 22'th amendment, <https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Rundfunkstaatsvertrag_RStV.pdf> accessed 6 February 2020

The Broadcast State Treaty in the version of his 22'th amendment, <https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/Rundfunkstaatsvertrag_RStV.pdf> accessed 6 February 2020

Announcement of a association ban against „linksunten.indymedia" from 14 August 2017 by the Federal Ministry of the Interior, BAnz AT 25.08.2017 B1, <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2017/verbotsverfuegung-linksunten.pdf?__blob=publicationFile&v=1>

Announcement of a association ban against „Altermedia Deutschland" from 04. January 2016 by the Federal Ministry of the Interior, BAnz AT 27.01.2016 B1, <https://www.bundesanzeiger.de/ebanzwww/wexsservlet?session.sessionid=141f108870e40a3a47f5e3e183ffd5d8&page.navid=detailsearchlisttodetailsearchdetail&fts_search_list.selected=f498931aa30af58c&fts_search_list.destHistoryId=58304>

Press release of the Federal Administrative Court from 30 January 2020, reference Nr. 05/2020, <https://www.bverwg.de/pm/2020/5> accessed 10 February 2020

Draft of the Federal Ministry of Justice and Consumer Protection from 19 December 2019,
<https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_BekaempfungHatespeech.pdf?__blob=publicationFile&v=1> accessed on 9 Febraury 2020

Draft of the Federal Ministry of Justice and Consumer Protection from 29 January 2020, Page 1, <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_NetzDGAendG.pdf?__blob=publicationFile&v=3> accessed 9 February 2020

Draft of the Media State Treaty from 5 December 2019, <https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/ModStV_MStV_und_JMStV_2019-12-05_MPK.pdf> accessed 9 February 2020

Form for reporting to the Federal Office of Justice, <https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/NetzDG/Service/Formulare/Meldung/Formular_node.html> accessed 5 February 2020

Facebook löscht täglich 1 Million Fake-Konten, <https://www.faz.net/aktuell/wirtschaft/facebook-loescht-taeglich-1-million-fake-konten-16635950.html?fbclid=IwAR0RP8jVr_94K4r2LeyCUtxqF7ENvn_3P-ydlPtsrt1ryleAB_bnlsBMTro&utm_campaign=GEPC%253Ds6&utm_content=buffercd02&utm_medium=social&utm_source=facebook.com> accessed 16 February 2020

BVerfG zum Recht auf Vergessenwerden I und II - Was bedeuten die Entscheidungen für Bürger, Gerichte und den EuGH? <https://www.lto.de/recht/hintergruende/h/bverfg-recht-auf-vergessen-europa-eugh-grundrechte-teil-2/> accessed 29 February 2020

LG Berlin: Teilerfolg für Künast gegen Online-Beschimpfungen, Redaktion beck-aktuell, becklink 2014911, beck-online.de accessed 4 December 2019

Case law

Federal Constitutional Court [15.01.1958] – 1 BvR 400/51, Federal Constitutional Court Report Vol. 7, 198

Federal Constitutional Court [05.08.1966] - 1 BvR 586/62, 610/63, 512/64, Federal Constitutional Court Report Vol. 20, 162

Federal Constitutional Court [22.06.1982] – 1 BvR 1376/79, Federal Constitutional Court Report Vol. 61, 1

Federal Constitutional Court [13.04.1994] – 1 BvR 23/94, Federal Constitutional Court Report Vol. 90, 241

Federal Constitutional Court [09.10.1991] – 1 BvR 1555/88 Federal Constitutional Court Report Vol. 85, 1

Federal Constitutional Court [24.02.1971] -– 1 BvR 435/68, Federal Constitutional Court Report Vol. 30, 173

Federal Constitutional Court, [16.07.1969] – 1 BvL 19/63

Federal Constitutional Court, [15.12.1983] - 1 BvR 209/83, Federal Constitutional Court Report Vol. 65, 1 – 71

Federal Constitutional Court [27.02.2008] - 1 BvR 370/07, Federal Constitutional Court Report Vol. 120, 274 - 350

Federal Constitutional Court [06.11.2019] - 1 BvR 16/13

Federal Constitutional Court [06.11.2019] - 1 BvR 276/17

Federal Constitutional Court [10.10.1995] - 1 BvR 1476/91

Federal Constitutional Court [22.05.2019] - 1 BvQ 42/19

Federal Court of Justice [27.03.2007] - VI ZR 101/06, published in: NJW 2007, 2558

Federal Court of Justice [19.04.2007] - I ZR 35/04, published in: NJW 2007, 2636

Federal Court of Justice [12. 11. 2009] - I ZR 166/07

Federal Court of Justice [22.07.2010] - I ZR 139/08, published in GRUR 2011, 152

Federal Court of Justice [12.07.2012] - I ZR 18/11, published in: NJW 2013, 784

Federal Court of Justice [12.07.2007] - I ZR 18 /04

Federal Court of Justice, [10.07.2015] - V ZR 169/14, published in: NJW 2016, 56

Federal Court of Justice, [22.02.2011] - VI ZR 120/10, published in: NJW 2011, 2204

Federal Court of Justice, [04.04.2017] – VI ZR 123/16, published in: NJW 2017, 2029

Federal Court of Justice, [14. 5. 2013] – VI ZR 269/12, published in: NJW 2013, 2348

Federal Court of Justice, [11.3.2004] - I ZR 304/01, published in: MMR 2004, 668

Federal Court of Justice [01.07.2014] - VI ZR 345/13 published in: MMR 2014, 704

Federal Court of Justice, [02.03.2010] - VI ZR 23/0, published in: NJW 2010, 1752

Federal Court of Justice, [11. 5. 2012] – V ZR 196/11, published in: NJW 2012, 2651

Higher District Court Munich [07.01.2019] - 18 U 1491/19Pre

Higher District Court Düsseldorf, [07.06.2006] - I-15 U 21/06, published in: MMR 2006, 618

Higher District Court Hamburg, [4.10.2017] – 5 W 75/16, published in: MMR 2018, 621

District Court Bamberg [18.10.2018] - 2 O 248/18, published on: <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-26648?hl=true> accessed 8 February 2020

District Court Frankfurt [10. 09.2018] - 2-03 O 310/18, published on:

<https://www.rv.hessenrecht.hessen.de/bshe/document/LARE190005792> accessed 6 February 2020

District Court Berlin, [09.09.2019] - 27 AR 17/19

District Court Berlin, [02.09.2019] - 27 O 433/19

District Court Würzburg, [7.3.2017] – 11 O 2338/16 UVR, published in: MMR 2017, 347

ELSA Greece

Contributors

National Coordinator

Thanos Kalaitzis

National Academic Coordinator

Stavroula Strati

National Researchers

Despoina Kotsi

Vasiliki Koukoula

Kriton Mygdalas

Athina Sotiriou

National Linguistic Editors

Despoina Kotsi

Vasiliki Koukoula

Kriton Mygdalas

Athina Sotiriou

National Academic Supervisor

Despoina Kotsi

Introduction

As it is known, the users of the internet are being increased every single day. If a person compares the number of the internet users from 2000 until 2020, they can reach the conclusion that the internet users have nowadays been at least doubled. It is definitely true that there are many reasons for this increase. The necessities of people to find out quickly information, to collaborate and to communicate with each other and to express their opinions are some examples. As far as the last concern, we need to highlight that during the last decade it has been becoming more and more common for the traditional way of information and communication to be abandoned. People stopped trusting television, radio and newspapers for their information and they started to prefer the internet. This choice had some other impacts, too. People wanted also to express their opinions via the Internet for two main reasons. The first one is that there is everyone's need for publicity. Thus, there is nowadays a need to create a social network profile, while it is easy for everyone to post something on the Internet, meaning that someone does not need the permission of someone else. To the contrary, if a person wants to express its opinion through the television or a newspaper, it is believed that this opinion will not be published, if it is not checked by the owner of the television channel or the owner of the newspaper. On the internet it is sure that this control does not exist, because everyone can post something on its Facebook page or its personal blog. The second reason is that through the Internet it is easier for someone to share its opinion about something with the others, to communicate with them about a matter and to exchange ideas. But we know that the coexistence of people in the traditional way of life has its collisions and needs to be regulated by the law in order to have a harmonic way of life. On the internet it is the same, as it is very common to insult a person, when someone expresses its opinions on the Internet. So, we need to find out if the Freedom of Expression via the Internet has some limitations, as the traditional means of information, or if the expression via the Internet is unregulated. And if there are some limitations, are they the same with them, which the government puts on the Press? And how can we balance the Freedom of Expression via the Internet with other fundamental rights of our co-citizens, in order to be the 'internet life' harmonic, too? (See question 11 in detail). These are some of the questions that we will try to give an answer on the following pages.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

Freedom of expression is protected in the Greek Constitution in the Article 14 paragraph 1 which states that 'Every person may express and propagate his thoughts orally, in writing and through the press in compliance with the law of the State'. The freedom of thought contains the shaping, holding, disseminating and obtaining of a thought.[823] Specifically the third form of freedom of thought is the freedom of expressing it, meaning the freedom to externalise it, to make it public to a certain number of people.[824]

The terms opinion and thought mean the intellectual or emotional reaction of a person to any external stimulus. That means that these terms concern not only the thought but also the feeling, not only ideas but also facts. A thought could be contained both in an Article and in a humorous story, both in a book and in a statement in the journalists. The right to express an opinion is preceded by the right to shape an opinion (first phase). It is forbidden for the State to intervene in someone's attempts to shape an opinion by exploiting its dominant position (for example the army) or through the media. The second phase of freedom of expression is the right to have and express an opinion without adverse consequences. The Constitution prohibits the dependence of the enjoyment of the civil and social rights. It also prohibits the creation of 'thought crimes'.

The third phase of the rights contains the freedom to express one's thought, to externalise it. It includes the right to choose the language as well as the time and place to express his opinion. The enumeration: orally, in writing and through the press is indicative. This externalisation can happen anyhow, so it also includes its' publication though internet. Finally, the fourth phase is the freedom to disseminate the opinion.

The Constitution also protects the silencing of an opinion, which means the right a person has to not express his opinion when he does not want to. This is a negative freedom of expression.

Freedom of expression in the Greek Constitution is not an absolute right, but it is subject to limitations. This is what the phrase 'in compliance with the law of the State' means. Everyone is free to express their thoughts as long as they are not violating other people's rights that the law is protecting. These laws refer to the general law of the State, those who protect a legal interest without going

823 Prodromos D. Dagtoglou, Constitutional law, Individual rights, page 342.
824 Ioannis Karakostas, Law and the Internet, page 39-40.

against neither other people nor to a specific opinion. Limitations to this right are also being imposed by the legal protection of other legal interests such as: morality, public order and safety, natural and cultural environment (Article 24 of the Constitution), pride (Article 2 of the Greek Constitution) and other rights of other people (for example the right to ownership which is protected in Article 381 in the Criminal Code).

Furthermore, the Freedom of Expression needs to respect the secrecy of communications as it is protected under Article 19 of the Greek Constitution. This means that information concerning secrets of an organisation for example cannot be published in a blog or online. [825] What is important is to distinguish between private and public persons. Private people have a lessened limit of judgment acceptance because they cannot reply that easily or support themselves and their personality, unlike public people.

A considerable exception to limitations constitutes the right of the blog owner has the right to make adverse judgments in order to inform the audience about something important concerning the public interest without legal consequences. This exception is posed by Article 367 paragraph 1 of the Greek penal Code which states that the adverse judgments and manifestations do not constitute illegal acts when they are being made due to a legal performance of duty, the exercise of legitimate force protection of rights or another justified interest.

With all these being said whoever violates the Freedom of Expression is violating the Article 14 of the Greek Constitution. The Freedom of Expression can be limited either when it is prevented or by when the fulfilment of this freedom comes with direct or indirect consequences for the person who expresses his thought. These two forms of limitations constitute censorship (prohibited by Article 14 paragraph 2 of the Greek Constitution) which is defined as the control exercised by an authority in the various manifestations of the thought and the art with the ultimate goal to prevent the exchange of information, ideas and opinions which are in contradiction with the principles of the authorities. Censorship is forbidden because as the Article 14 states, the thought is free and cannot be limited unless it violates a law.[826] The right to express freely a thought is closely linked with the right to information, not only on its' active form (the freedom to inform) but also on its' passive form (the freedom to be informed) because the right of expressing a thought would have no reason to exist, if the right to receive or to accept it did not exist. The right to information is protected though separately from the right to express an

[825] Freedom of Expression and anonymity online, Journal Media and Communications Law, issue 3/2011.
[826] Prodromos Dagtoglou, Constitutional law, individual rights, page 364-65.

opinion the right to information is protected under the Article 5A of the Greek Constitution which states that: All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties.

All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of Articles 9, 9A and 19.

The active form contains the right to inform others. On the contrary of the freedom of thought, the distinction between correct and misleading news is important. The right to spread misleading news is not protected under the Article 5A and if someone does that is accountable under Article 14 paragraph 1 citation b 'in compliance with the law of the State' because such a law is the Article 191 of the Criminal Code who punishes 'Anyone who publicly or through the Internet disseminates false news in any way that may cause fear to an indefinite number of people or a certain circle or category of persons, who are thus forced to perform unscheduled acts or to terminate them, with the risk of being harmed in the country's economy, tourism or defence capacity or to disrupt international relations, is punishable by up to three years in prison or a fine. Anyone who negligently becomes guilty of the act set forth in the preceding paragraph shall be punished by a fine or by the performance of public service.

The passive form contains the right to be informed, meaning the search, gathering and receiving information without having a necessary goal of informing others. Information is considered every object of knowledge. The freedom of information though does not guarantee access to all sources of information but mainly to the generally accessible sources of information, meaning the sources that are addressed to the public. In this context the practice of hacking is not a protected freedom of information[827]. Every limitation is in contradiction with the free access to generally accessible sources of information, such as the denial of access or the concealing or distorting of information.

There are though some legal limitations, those from the Article 14 who apply analogously here as well. Specifically, one of them is the privacy of communications which is protected under Article 19 in the Greek Constitution. This protection is irrelevant from the way or the compliance or not with the legality of acquisition of the confidential information. Other limitations of the

827 Ioannis Karakostas, Law and Internet, , page 4.1.

freedom to information include the protection of the effective investigation of crimes or administrative offenses.

The second paragraph protects the access to the information society. The provision not only recognises a right to information but also introduces an obligation of the State to ease the access to information. The right to electronic information, as it is protected under Article 5A, paragraph 2, and citation 2 is analysed in two individual rights: the right to access and the right to develop the electronic information. The right to access the electronic information is also protected under Article 14 paragraph 1, but in Article 5A has some specific manifestations such as the prohibition of sending uncaused messages from the state to the citizens (spamming) as well as the safeguard of citizen's right to access in the internet, to use a specific language or to view a specific content.[828]

The protective scope of this regulation also belongs to the right of unhampered electronic communication through the free access to free navigation in the internet. The right to public free communication mostly refers to the free participation in newsgroups and chats.

There are certain limitations for this right too as stated in the Article 5A, paragraph 2. Specifically, the right to electronic information has boundaries: the inviolability of home and of private life (Article 9) which prohibits a person to use electronic collect of information in order to monitor someone's personal life and trap someone's computer. Furthermore, the collection, processing and use of personal data with electronic means are protected already under Article 9A of the Greek Constitution. The secrecy of correspondence is protected under Article 19 paragraph 1 and it co applies with Article 5A and the information society, firstly concerning the safety of the telecommunications networks and secondly concerning the reassurance of safe exchange of information packets.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

In Greece there is no specific regulation targeting the blocking or taking down of internet content but many various Articles in different legal documents. One of these is Article 66E Law 2121/1993 concerning the violation of intellectual property rights. This Article foresees the creation of a Committee charged with the work to determine if there is a violation (after the holder of the violated right

828 Ioannis Karakostas, Law and the Internet, page 34.

submits an application) and if there is the Committee calls on the addressees of the decision to comply with it.

As was mentioned above, the Article 14 can analogically apply for the expression though the internet, because the enumeration was non-exhaustive. That means that when the freedom of expression violates the law or the rights of others it can be limited. The practice of seizure cannot apply in the case of the internet, but other means of punishment can. The same exceptions apply for the prohibition of censorship.[829] Firstly, though some other things must be said. In order for an illegal content to be filtered or taken down some requisitions must fulfil: the intermediaries must have knowledge of the content being shared though their page. Intermediaries are the entities who perform as go between for the transmission of information. There are the only ones capable of taking down, filtering or blocking internet content. But in the Greek civil law in order to be held responsible indirectly for an illegal content there must be knowledge of the content on behalf of the intermediaries.

Specifically, in the Greek Presidential Decree 131/2003 adopted in the lines of the Directive 2000/31 it is stated that the liability of the intermediaries can be judged by a Court or an Authority and decided of the termination or prevention of any illegal activity. This measure could require the cease of access to illegal information. Although not specifically defined under the law, the Authority could be the Hellenic Data Protection Authority (HDPA (which judges violations of the rights protected under GDPR Regulation, violations of the provisions concerning unwanted calls for promotion of products or services and the delivery of unwanted emails – Article 11 paragraphs 1 and 2 of the Law 3471/2006), the Hellenic Authority for Communication Security and Privacy (HACSP) – an administrative authority which judges violations of the constitutional rights on the secrecy of communications- or the National Telecommunications and Post Commission (NTPC) - which judges complaints concerning communication services.

Concerning the type of procedure before the Court, the Greek Law allows an injunction procedure in front of the First Instance Civil Court.[830] In order for the injunction to be obtained though, is that 'the information society tights must seem under threat of infringement. Specific areas are covered from different sources of law. For example, the copyright infringements are covered from the Greek Copyright Law 2121/1993, Articles 64 and 64A which are harmonising

829 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, Greece.

830 Articles 682 of the Greek Code of the Civil Law Procedure.

the Copyright Directive 2001/29 Article 8 paragraph 3 and Enforcement Directive 2004/48 Article 11.

The trademark law provisions are similar. According to Articles 153, 154 of the Greek Law 4072/2012 the holder has the right to seek an injunction ordering the confiscation of products that have the violated sign or the provisional blocking of distribution.

Apart from these though there are several cases that are being dealt with from different Greek laws. For example, concerning the child pornography, the issue is regulated in Article 18 in Law 4267/2014 which states that the Public Prosecutor has the right the elimination of a hosted website in Greece that ether contains either transmits child sexual abuse images. In case the website is not hosted in Greece or elsewhere the Public Prosecutor may order the blocking of access to such websites. The order has to be fully justified in these certain circumstances and has to be addressed to the owner of the website and the National Telecommunications and Post Commission (NTPC). The NTPC has to notify all access providers registered in Greece, according to the Greek Telecommunication Law (4070/2012). There are no other provisions regulated the blocking of access about other crimes and they are regulating by the general provisions.

Furthermore, concerning the gambling, the Greek Gaming Commission is an independent authority which is charged with the publication of blacklisted gambling sites. According to the Law the access to these sites must be disabled from the internet provides in Greece. According to Article 3 paragraph 4 of the Internet Gambling Regulation, blocking must happen when the access is attempted through 'an IP address residing in the Greek territory'. In addition, Internet Service Providers must not allow 'any action of commercial communication' between the illegal gambling providers.

The majority of cases that the Courts have dealt with, concern copyrights and demanded the intermediaries to block access to sites that violated the copyright law. Although there are few equally important cases concerning the freedom of expression online.

The most known is the case of 'Father Pastitsios' a satirical Facebook page that seemed to satirise a dead Orthodox priest, who according to the belief of some faithful, has uncanny powers of perception. After many complaints and a raise of the issue in the Greek Parliament from a member of the far-right party the police lifted the secrecy of correspondence and arrested the manager of the page. Afterwards in the decision 5635/14 of the First Instance Court of Athens he was convicted to four months of prison for insulting religions, and especially for

violating the Article 199 of the Penal Code 'whoever, publicly and maliciously insults anyhow the Eastern Orthodoxy of Christ or any other tolerated religion in Greece is being punished by imprisonment of until 2 years'.

He was later acquitted on the appeal trial but not for substantive grounds but because his crime was time-barred. Since there is no specific legislation regulating the crimes committed through the internet the general provision applied here. Finally, though, Facebook took down his page.

In the case 4658/2012 the Court ordered the national access providers to temporarily block the access to their subscribers to the IP addresses corresponding to some websites because the content being shared there was massively violating the provisions of the Intellectual Property rights. This decision was held after the petition of five collecting societies. Furthermore, the Court decided that a general blocking of access in order to protect the IP rights would be disproportionate since the violation occurred on specific websites and would not be in accordance with the Article 5A paragraph 2 of the Greek Constitution (information society).

On the contrary, in the case 13478/2014 the Court did not grant the injunction. Five big collective organisations lodged a petition asking that some host providers would block the access to the websites where products of intellectual property were being shared (music and movies). The, taking into consideration the Greek IP law (2121/1993), the Presidential Decree (131/2003) and the Greek legislation about the secrecy of communications stated that the intermediaries cannot be held liable because they do not have such an active role in the origin nor the destination neither are they aware if the content being shared is illegal and therefore they are protected under Article 13 of the Presidential Decree 131/2003 in their website and therefore they are not responsible. Furthermore, the Court decided that according to Article 14 of the PD the defendants did not host the illegal content and since it was transmitted though forums or hyperlinks and therefore a blocking of information wouldn't limit in the illegal conducts but would also cover the legal ones, imposing a general obligation for the providers to control all the transmitted contents. In addition, the blocking measures operate automatically, and they cannot distinguish between legal and illegal and therefore this filtering method could certainly not apply. Furthermore, the adoption of a measure like this would be in contradiction with the Article 5A paragraph 1 (freedom of information), Article 5A paragraph 2 (freedom of information society), the right to protect personal data (Article 9), the right to secrecy of communications (Article 19) and

the principle of proportionality.[831] The regulation of online blogs is also very interesting. More specifically the online blogs are also a subject of Article 14 of the Greek Constitution and therefore the same limitations apply as cited in paragraph 2. Regarding the right to personality the intermediaries are not responsible for insulting comments. They may have to intervene though in such comments or uploads either in a preventive or in a suppressive way. Concerning the responsibility of the intermediaries in this case the Greek case law has delivered controversial decisions.

In decision 44/2008 of the First Instance Court of Rodopi, the case was about insulting through blog. In this case the Court subjected the blogs in the provisions for the press and stated that they apply analogically. For this reason, it ruled according to the Article 681 of the Greek Code of civil Procedure. Furthermore, it granted the immunity of the hospitality (PD 131/2003) to the intermediary company and it attributed no responsibility to her. They could not find the identity of the actor of the insult.

In case 4980/2009 of the Court of First Instance of Peiraias judged again a case of insulting the personality in a blog. It concluded that blogs are not subject to the provision of the Press for three reasons. Firstly, the user of the internet wishes only to express his opinion and therefore does not wish for it to spread. Secondly, the user normally cannot afford to pay the fines that the Press legislation demands and thirdly usually he is not under the auspice of a higher financially independent publisher who is responsible in an objective way, as the press legislation anticipates. Furthermore, the Court concluded that blogs have neither the business nor the hierarchical structure of a press and therefore they cannot be considered as press and the press provisions cannot apply. It additionally considered, taking into consideration the Article 13 of the PD 131/2003 that a distinction between anonymous and well known editors shouldn't be made.

In the case of the First Instance Court of Thessaloniki 25552/2010 the Court also occupied with an insult a blog. It rules that a blog constitutes a space of opinion exchange and the owner of the blog cannot decide who will enter and write in it neither the comments that will be displayed and therefore conclude that an analogical application of the Press provisions would cause a socially unbearable outcome. Additionally, it ruled that if someone seeks protection in this context, then this has to be traced in the general provision of the Civil Code, which protects the personality (Article 57, 59, 914, 932).

831 George Giannopoulos, The responsibilities of online service providers, page 274-77.

In case 22228/2011 of the First Instance Court of Thessaloniki the Court had to deal with the insult of the personality with a famous journalist being included. It concluded that blogs haven't the purpose of transmitting news for the people to gain knowledge which is the main object of the Press rather the exchange of the knowledge, opinions and ideas from a dynamic structure of communication. For the rest it agreed with the previous decision stating that blogs have neither the business nor the hierarchical structure of the Press and furthermore no superior financially independent person aides the blog users.

In case 164/2011 of the Second Instance Court of Athens the Court agreed with the first decision stating that the provisions of the press also apply in the case of insult through a blog. In contradiction with the previous decisions though, it applied Article 4 paragraph 10 of the Law 2328/1995 in the electronic insults as well, which imposes a higher responsibility for the press for the broadcasting channels of national and regional scope and it also foresees a minimum amount of compensation. That means that the Court expected from the intermediary to be able to determine when a post was violating the law and to act accordingly with respect to the laws.

Regarding the responsibility of the host of hyperlinks Greece has also not a specific legislation and therefore the responsibility of the hosts can be traced either in other provisions or in the case law. There are three important cases for this issue: the first, in the Three Member Magistrates in Kilkis 965/2010 ruled that the placements of links which lead to published work in other websites does not fall under the term produce or public performance of the Article 3 of the Law 2121/1993 unless the owner has received special measures of protection of his work or a limitation of a required permission exists.

On the contrary decision 4042/2010 of the First Instance Court of Athens ruled that an owner of a radio broadcast website which refers to a website of a third person proceeds to an audio presentation of the work. He therefore makes the work accessible to the audience without the permission of the owner and violates the copyright law. Another interesting decision the 13/2011 of the Authority of Personal Data Protection ruled that it is better to use hyperlinks for the page of ASEP because the copy with the method of copy and paste has the hazard of inaccuracies and publication for a longer period than the required time for the process of the personal data. In case the content of the website in which the hyper-link refers to changes the intermediary has to be aware of this change in order to establish responsibility.

Another important issue concerns the freedom of expression and the right to anonymity online especially in blogs. Although generally anonymity is protected

as a right which belongs in the private sphere, it could also violate some other people rights. This mainly happens when the anonymity is misused in order to insult someone or violation of the private sphere. In the Greek legislation the obligation to brand the blogs is not an unknown issue. For example, in law 3783/2009 the opportunity to use the phones anonymously has been aired in order to protect the public order and safety.

Generally, it would be better for the blogs owners to reveal their identity because of reasons of general interest (for example the protection of the rights of the insulted against defamatory comments) and both the core of the rights and the principle of proportionality are not violated because there are no moderate measures.[832]

Another interesting case concerns the use of emoticons on Facebook comments. In the case 174/2017 the First Instance Court of Volos convicted the accused for insulting post against the accuser to stop occupying with her with any way, though an injunction decision. The same court later in the decision 1456/2018 convicted again the accuser because he used a laughing emoticon in a post of the accuser, violating therefore the previous decision. The Court considered the emoticon as a comment with an insulting content which leads to a violation of the right to personality.[833] This is strengthened and was evaluated by the whole behaviour the accused had towards the accuser.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

The Freedom of Expression is of course one of the fundamental requirements for the prosperity of democracy and the progress of every single person. According to the European Convention of Human Rights, freedom of expression, however, is not absolute. In some circumstances the state can restrict this freedom, regardless of the way, by which the opinions and the ideas are expressed. This means that the state can put restrictions to the right to freedom of expression, even if the person expresses its opinions via the Internet.[834] The word 'reconcile', also, that the Regulation uses, indicates the fact that neither the freedom of expression nor the protection of personal data are absolute rights. That means that the legislator can put restrictions on them, and the judge of

832 Freedom of Expression and anonymity online, Journal: Media and Communications Law, issue 3/2011.
833 Freedom of Expression and anonymity online, Journal: Media and Communications Law, issue 3/2011.
834 M.D. Papadopoulou, 'ECHR decision of 19.02.2013 case *Neij and SundeKolmisoppi v. Sweden* No 40397/2012 [transfer of documents in Internet]' (2013) volume 1 Law of media and communication 100.

every case shall harmonise ad hoc the aforementioned rights.[835] The judge can have the use of some tools in order to be helped in harmonising and the most important of them is the principal of proportionality.[836]

This principal has been already known in Greek case law since 1984, when the Council of State decided that the restrictions, which the legislator or the administration puts on the exercise of a right in order to achieve an aim shall be suitable and necessary for achieving this particular aim.[837] Since 2001, the principal of proportionality is officially part of the Greek constitution.[838] Of course, as far as the moral judgments are concerned, we need to clarify that they cannot be forbidden, because they are part of the right to freedom of expression. Exception to this rule is accepted, when it is about offensive comments; they are not included into the right to freedom of expression.[839]

So, the control of proportionality consists of three individual steps. The first one is the suitability of the restriction. If the restriction is irrelevant to the aim that the legislator pursues, then the control is over and the law that introduces this restriction is unconstitutional. During the second step the judge has to research if the restriction is necessary in order to the aim of the legislator to be achieved. The condition of necessity is met, when there is no other way, which would restrict the right less than the way that is actually chosen, for achieving the aim. Again, if the judge finds that the restriction is not necessary, the control is over, and the law is against the constitution. At the final step the restriction shall be *stricto sensu* reasonable, considering the competing interests of different groups at hand; an analysis between the costs and the benefits is taken place and the benefits of the restriction shall be more than the costs. Only if all these conditions are fulfilled, is the restriction constitutional.[840]

To this point we can refer to the fact that the Greek legislation is in accordance with the European Convention of Human Rights (ECHR) and the case law of the European Court of the Human Rights. This is, because in Article 10, paragraph 2 of ECHR, which refers to the restrictions that can be put on freedom of expression, the principal of proportionality is provided. The judges of the European Court of the Human Rights are the only responsible to find out, if the principal of proportionality is satisfied. So, they control, if the following five requirements are fulfilled: a) if the conviction of a person for

835 Leonidas Kotsalis and KonstandinosMenoudakos, *GDPR* (first published 2018, NomikiBibliothiki) 74.
836 Leonidas Kotsalis and KonstandinosMenoudakos, *GDPR* (first published 2018, NomikiBibliothiki) 77.
837 'Council of State 2112/1984', The Constitution, (1985) 63.
838 Greek Constitution Article 25, paragraph 1.
839 *ApostolosTasikas*, 'Redress of the infringement of personality (in liability of offensive comments of posts on Internet) rights' (2019) volume 3 Law of media and communication 309.
840 Kostas Xrysogonos*, Individual and personal rights* (1st supp, 3rd ed, NomikiBibliothiki 2006) 90-94.

infringement of the intellectual property rights or the personal data of someone or for violation of some Articles of the penal code which refer to the reputation of someone constitutes restriction to freedom of expression, b) if this restriction is provided by the law, c) if the legislator aims to achieve a legitimate purpose, d) if this restriction was necessary in order to this purpose to be achieved and e) if between the restriction to the right to Freedom of Expression and the legitimate purpose exists *stricto sensu* reasonableness.[841] So, we can reach to conclusion that both the European Court of the Human Rights and the national Greek courts apply in the same way the principal of proportionality.

Keeping this information in mind, we can refer to some cases, in which the Greek case and jurisprudence made an effort to offset the right to online Freedom of Expression and the right to the protection of personal data. A significant parameter that is taken into account is the following: if the person, whose rights are violated, is a public person, then according to the principal of proportionality the right to freedom of expression takes precedence over the right to protection of personal data. So, the question is who a public person is. It is about a general term, which includes several types of people, such as politicians, musicians, journalists, artists.[842]

Another criterion that the principal of proportionality takes into account is the nature of the data that are made publicly known. The control of proportionality is stronger in the field of sensitive data. There is some sensitive data that is so strongly connected with the nature of human personality, which only under exceptional cases can be made publicly known, even if they refer to politicians. In this case, the control of proportionality is even stronger, if the disclosure of sensitive data takes place on a website, which has many visitors.[843]

In addition, there are some other factors that need to be born in mind. A determinant factor is the way under which a person holds information. If the information is acquired in an illegal way, then the person who holds it, cannot upload it.[844] It is about circumstances, such as the acquisition of the information by the use of a hidden camera or by theft of telephone calls or e-mails. But there are some exemptions. If person A, who has acquired illegally the information,

841 M.D. Papadopoulou, 'ECHR decision of 19.02.2013 case *Neij and SundeKolmisoppi v. Sweden* No 40397/2012 [transfer of documents in Internet]' (2013) volume 1 Law of media and communication 100.

842 Leonidas Kotsalis and KonstandinosMenoudakos, GDPR (first published 2018, NomikiBibliothiki) 74-75.

843 Leonidas Kotsalis and KonstandinosMenoudakos, *GDPR* (first published 2018, NomikiBibliothiki) 76.

844 41/2017 decision of the Authority of Personal Data Protection.

gives this information to person B, then the last one can upload them, unless that person is aware of the illegality.[845]

At the harmonisation of the Right to Freedom of Expression and the right to protect personal data, it is also highly significant the accuracy of the personal data that someone wants to upload. The importance of accuracy can be found in the fact that the personal data that someone has uploaded might not be actually true after a period of time. For example, the publication of the information by a journalist that a public person has committed a crime might be rightful. But, if the court finds that public person not guilty, then the journalist is obliged to publicise the decision of acquittal.[846]

Let us refer to a case, with which the Hellenic Data Protection Authority has dealt. The facts are the following: a citizen A denounced the mayor B of the town for posting on its Facebook page that the citizen A receives a disability pension. The mayor B replied that the citizen A has posted on a local blog, which the citizen A administrates, a slanderous comment that the mayor B defrauded the local community. The mayor added that it is known to the town that the citizen A receives disability pension and that he or she has posted that information on Facebook as a person and not as a mayor. The citizen A claimed that the mayor shall not disclose its private sensitive data. The mayor B asserted that the comment on Facebook was posted because of a harsh criticism of the citizen A. Moreover, the citizen B added that aim of the comment was to refer to the status of the citizen A as a retiree and to the right of that person to receive pension. The information that this citizen receives pension because of disability and not because of old-age does not violate that person's sensitive data. And this is, because the mayor has not referred to the details of the retirement, such as to the term, the sum and the requirements of the pension, so the sensitive data has not been violated.

The decision of the Hellenic Data Protection Authority was the following: The disclosure of the information that someone receives pension is included in the sensitive data. Moreover, the processing of personal data is not illegal, if this information is being processed for domestic use. If the personal data are being processed by a user of social media in order to its political aims be achieved, then the user has the liability of a processor, who discloses the personal data to the social media itself and to the other users, who are using the social media. So, the user needs the consent of the person, whose sensitive data wants to disclose,

845 Leonidas Kotsalis and KonstandinosMenoudakos, *GDPR* (first published 2018, NomikiBibliothiki) 76.
846 Leonidas Kotsalis and KonstandinosMenoudakos, *GDPR* (first published 2018, NomikiBibliothiki) 76-77.

in order for that disclosure to be legal. In addition, if the user has many friends on Facebook, or the information that he or she posts is available not only to the friends, but also to other users of that social media, it is an indication that the social media is not used for domestic purposes and the user is a processor. In our case the mayor had more than 1000 friends on Facebook and its posts were available to everybody, not only to its friends. Additionally, the mayor was using Facebook in order for the citizens of the town to be well informed. So, the mayor is a processor and did not receive the consent of the citizen A in order to disclose the sensitive data of the last person. So, the Hellenic Data Protection Authority decided that the post of the mayor was illegal and obliged the mayor to delete the post on Facebook in five days and not to repost it again in the future.[847]

We can now refer shortly to some other important decisions of the Hellenic Data Protection Authority. According to the decision 17/2008, the posting of photos of the erotic life of a person without its consent constitutes illegal process of its sensitive personal data and is contrary to Article 8 of the ECHR.[848] As far as the publication of court decisions concerned, in the opinion of the Authority, is this publication legal only if the personal data of the natural persons are erased. If they are not erased, then the publication is contrary to Article 9A of the Greek Constitution and the Article 8 ECHR, as the publication on the Internet of personal is connected with a lot of risks. Furthermore, the publication of the case is necessary in order for everyone to be informed, but the protection of the personal data shall be taken into account, too.[849] With regard to the publication of the taxes on the Internet that some debtors owe to the State, firstly the Authority had the opinion that it is contrary to Article 8 ECHR. Moreover, the combat of tax evasion is not a legitimate purpose.[850] Later, the Authority changed its mind and now has the opinion that the aforementioned publication on the website of the Minister of Finance is legal, if some requirements are met, such as the finalisation of the tax liability and the prior written notification of the debtor that the publication will take place.[851]

Now we can refer to a case by which someone has been convicted for libel. The facts are the following: the person A works for a legal person governed by the private law, he is married to his colleague and from 2008 he is the president of the trade union of the legal person. A Greek Minister accused the person A that he took advantage of his post in order to serve the interests of his family

847 17/2016 decision of the Authority of Personal Data Protection.
848 17/2008 decision of the Authority of Personal Data Protection.
849 2/2006 decision of the Authority of Personal Data Protection.
850 1/2001 opinion of the Authority of Personal Data Protection.
851 4/2011 opinion of the Authority of Personal Data Protection.

members, meaning that he was using non-transparent methods in the performance of his duties. The court found the Minister guilty of libel, as he posted the aforementioned information on his Facebook page, even though the Minister knew that the information was not true. According to the Article 57 of the Greek civil code an infringement of personality can take place when the criminal act of libel has been conducted. There is no difference if the libel has been conducted through an Article in a newspaper of via a post on the Internet. To the contrary, the second situation is even worse, because the internet content is available to more people. So, the court obliged the Minister to delete his post from his Facebook page and moreover to post on it the decision of the court.[852]

Furthermore, the unlawful internet content, which is illegal under civil law, is not treated in the same way as the respective unlawful content under the criminal law. For example, if someone infringes the personality of someone else, by posting the personal data of the last one on the Internet, the offender will not be treated in the same way by the two parts of the law. The difference between the civil and the criminal law is that in the first one the liability of the tortfeasor is strict,[853] as far as the cessation of the infringement and the non-recurrence thereof in the future concerned. But in the last one the offender must be liable in order to be found guilty. The criminal liability of the offender is provided in three Articles in the Greek criminal code: The Article 361, which refers to the crime of insult, the Article 362, which refers to the crime of libel and the Article of 363, which refers to the crime of defamation. In the Greek civil code, the protection of personality is provided in the Article 57. According to this Article, the injured person can file a claim with the court with the following petitions: a) the ascertainment the infringement of personal data, b) the legal redress of the infringement with a statement from the tortfeasor, which will be posted on the Internet and c) the termination of the infringement and the restoration of the situation existing previously. So, the difference between the civil and the criminal law is significant, because under the civil law the injured person does not need to prove that the tortfeasor was liable. But if the injured person wants to file a claim for compensation, according to the provisions about tort, then this person needs to prove the liability of the tortfeasor. So, in this last situation the liability of the tortfeasor is not strict.[854]

852 6827/2018 Court of First Instance of Athens.

853 Apostolos Georgiadis, General part of the Greek civil code (1st supp, 4th ed, Sakkoulas 2012) 180.

854 G. Giannopoulos, 'ECHR decision of 4.12.2018 case No 11257/16 (fourth part) [Liability from the use of hyperlink]' (2019) volume 1 Law of media and communication 52 ,

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

We could say that the issue of blocking and taking down internet content is not self-regulated by the private sector in Greece. There is no internet code of conduct, so we will focus on the proposals that have been made on this field.

The Internet provides a lot of possibilities of instant response when an infringement of personality takes place. This is the reason why many proposals have been made on the field of Internet self-regulation. Some of these proposals are the following: a) the use of filters which immediately take down internet content that contains offensive words, b) marking of websites with content that violates the law and binding this marking with the search engines, c) supervision of the posts that are being made on the internet and taking down the offensive internet content immediately or after notice, d) adoption of internet code of conduct and adoption of mechanisms of alternative dispute resolutions, etc.[855] An internet code of conduct has been proposed by the Greek theory, but it has not been enacted as a law.[856]

Moreover, an important matter is if the possibility to respond to an offensive post is an adequate and appropriate way of dealing with illegal internet content. The European Court of Human Rights has decided that the possibility of response is not enough, even though if there is a system of taking down offensive posts after notice. And the reason is that a post on Internet is not easy to be deleted, it is accessible to many people and a single person is not able to control the huge volume of internet content in order to find out if an offensive comment has been made against him or her. This is a job that the owners of the website need to do.[857] The single persons have neither the method nor the funds for such a control.

Although there is no internet code of conduct generally, there is a code of conduct of digital media. This code makes it clear under which circumstances the posts that the journalists make on the Internet should be taken down or corrected by the journalists by themselves. For example, let us say that a person is accused of a crime and a journalist makes a post on the Internet about it. If charges are withdrawn, then the journalist should add this development to its post, but not erase it. The journalist should also do the same, if there is a proven

855 Kostas N. Stratilatis, 'Is the public sphere of the Internet needed a specific regulation?' [2014] Newspaper of Administrative Law 94.

856 Basilis Sotiropoulos, 'Blogs' code of conduct', <http://elawyer.blogspot.com/2007/03/blog-post_6732.html>.

857 Delfi v EsthoniaApp no 64569/09 (ECHR, 16 June 2015).

acquittal of the accused. And finally, if the post contains inaccuracies, the journalist should mention the inaccuracy to its post and not erase it and rewrite it. The code explains deliberately how the journalist should reconsider its internet text in order for the citizens to be well informed.[858]

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

As regards the application of the Greek law, it is noted that before 25/05/2018, when Directive 95/46/EC had actually been in force into the Greek legal order by Law No. 2472/1997, the National Authority for Data Protection had the jurisdiction to examine all relevant matters. The Directive 95/46/EC was repealed on 25.05.2018, when the Implementing Regulation (EU) 2016/679 under the name 'General Data Protection Regulation' (hereinafter referred to as GDPR) has been introduced. [859]

To transpose the recently-introduced EU legislation into the national legal order, the Greek Law No. 4624/2019 entitled 'Data Protection Authority, implementing measures of the European Regulation (EU) 2016/679 of the Parliament and the Council of 27 April 2016 on the protection of natural persons against the processing of their personal data; and transposition into the national law of the European Directive (EU) 2016/680 of the Parliament and the Council of 27 April 2016 and other provisions' was voted by the Greek parliament and was published in its Government Gazette (Government Gazette A137/29/08/2019). With the General Data Protection Regulation ('GDPR') already in force, the national applicable law, whose voting was delayed long enough, specifies some of its settings and takes advantage of the benefits provided by the GDPR providing for more specific arrangements at national level.

According to the latest national legislation under the Law No. 4624/2019 that incorporated GDPR, there exists a specific provision in Article 34 about the right to delete, which could be characterised as being of a restrictive nature since the ad hoc legislative provision states that; if the deletion in the event of manual processing is not possible due to the particular nature of the storage process or the deletion is possible only by a disproportionate amount of effort and the data

858 Code of Conduct of digital media', <http://www.ened.gr/Content/Files/ENED_OTHER_FILES/ENED-CODE-OF-ETHICS.pdf>.

859 Regulation 679/2016 (EU) of the European Council and of Council of 27 April 2016 on the protection of natural persons against the processing of their personal data and the free movement of such data; and repealing the Directive 95/46/EC (General Regulation on Data protection).

subject's interest in the deletion is not considered significant, the right of the subject and the obligation on the part of the controller to delete personal data in accordance with Article 17(1) of the GDPR shall not exist. This includes also the exceptions to the obligation to erasure referred to in Article 17(3) of the GDPR, i.e. the exercise of the right of Freedom of Expression and Information, compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, reasons of public interest in the area of public health, the establishment, exercise or defence of legal claims;[860] and the case in which the deletion would conflict with legal or contractual retention periods as referred in Article 17(1)(a).[861] In all these cases, the deletion shall be replaced by the restriction of processing in accordance with Article 18 of the GDPR. However, the above exceptions shall not apply if the personal data has been illegally processed.[862]

Also, the national provision states in the second paragraph of Article 34 of the national Law in question that in addition to Article 18(1) (b) and (c) of the GDPR that refer to cases falling under the right to restriction of processing,[863] the

860 Article 17 GDPR, The Right to Erasure ('Right to be Forgotten'): '1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d) the personal data have been unlawfully processed; e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: a) for exercising the right of Freedom of Expression and information; b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or e) for the establishment, exercise or defence of legal claims'.

861 Greek Law No. 4624/2019, Article 34, paragraph 3.

862 Greek Law No. 4624/2019, Article 34, paragraph 1.

863 Article 18 GDPR - Right to restriction of processing: 'The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (...) b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction

exclusion of the obligation to erasure and, thus, the replacement by the so-called restriction method shall apply mutatis mutandis to Article 17(1) (a) and (d) of the GDPR, to the extent that the controller has reason to believe that the deletion would be detrimental to the legitimate interests of the data subject. The controller shall inform the data subject of the limitation of the processing if such updating is not impossible or does not entail a disproportionate effort.[864]

All in all, Article 34 restricts the right to delete personal data and the corresponding obligation of the controller in accordance with the Article 17 paragraph 1 of the GDPR. However, the derogations referred to in Article 17 paragraph 3 of the GDPR remain unaffected by the provision. The setting applies both to public and private operators. Subject to the conditions set out in paragraphs 1 to 3, deletion is replaced by the restriction (Article 18 of the GDPR). Through the measure of the restriction the right or obligation to delete personal data is delimited to the extent required by Article 23(2) (c) of the GDPR.[865] Further, Article 18(2) and (3) and Article 19 of the GDPR provide effective safeguards against the cases of abuse and misstatement of the meaning lying under the Article 23(2) (d) of the GDPR. Exceptionally, the case to impose a restriction on processing in accordance with Article 18 of the GDPR instead of deleting, does not apply where personal data have been unlawful processing, since the person responsible for the illegal processing of personal data is not worthy of protection and cannot be based on disproportionate attempt to remove the storage type selected by it. The first subparagraph of paragraph 2 places the restriction method for the benefit of the protection of legitimate interests of the person to whom the personal data relate in accordance with Article 23(1) (h) of the GDPR.[866] In accordance with Article 18(1) (b) of the GDPR the restriction of the unlawful processing of personal data is done only at the request of the subject of the data. Furthermore, Article 18(1) (c) of the GDPR allows the restriction of processing when the controller no longer needs the personal data for processing purposes, but these data are required by the

---

of their use instead; c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (...)'

864 Greek Law No. 4624/2019, Article 34, paragraph 2.

865 Article 23 GDPR – Restrictions: '1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society (...) 2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to: (...) the scope of the restrictions introduced; (...)'.

866 Article 23 GDPR – Restrictions: '2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to: (...) h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction'.

subject to establish, practice or support claims. On the contrary, paragraph 2 of Article 34 of the national law provides, even without a corresponding request by the person concerned, a general obligation of restriction by the person responsible if the latter has a reason to believe that the removal of the data will affect the subject's legitimate interests. The relevant setting is necessary because the person responsible is, in principle, obliged under the Article 17 of the GDPR not to delete unnecessary or illegal processing data. Paragraph 3 provides for a restriction in the event when the deletion of the personal data is no longer required because it runs counter to legal or contractual periods of conservation. The exception protects processors from conflict tasks.[867]

b) Another specific provision in Article 35 about the 'Right to Object' to processing of personal data, which by the GDPR definition also includes the storage and making available of any personal information.[868] According to the letter of the law, the right to object to the processing does not apply to a public body if there is an overriding public interest in the processing, which goes beyond the interests of the data subject or a provision of law obliges the processing to take place.[869]

All in all, Article 35 restricts the right of the subject of personal data to object before a public body in accordance with Article 21(1) of the GDPR, in part because the processing is imposed by a public interest which overrides the interests of the subject of the personal data; or this is required by law. The Article presupposes a public interest on the part of the controller within the meaning of Article 23(1) (e) of the GDPR.[870] This must be specific in the given case and take precedence over the interests of the subject of the personal data. In addition, the right to object is excluded if there is a legal requirement for processing. The Article 29(4) and the Article 30(2) contain specific restrictions relating to the

867 Explanatory Memorandum to the Law No. 4624/2019, pp. 26-27.

868 Article 4 GDPR Definitions - 'For the purposes of this Regulation: (...) 2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (...)'.

869 Greek Law No. 4624/2019, Article 35, paragraph 1.

870 Article 23 GDPR – Restrictions: '1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (...) e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (...)'.

right to object to the processing of personal data for archiving purposes for the public interest and for research, scientific, historical and statistical purposes.[871]

In this regard, the Hellenic Authority for Data Protection has also developed its very own res judicata; in the past, the Authority has confirmed that the request of the applicant to remove specific data had been legally justified on the basis of the assessment of the above legal criteria, taking into balanced account the overriding nature of the public interest.

A case was brought before the Authority by a person holding a position in the Hellenic Aerospace Industry seeking the removal of specific links, which appear in search results based on the applicant's name, which mostly lead to publications referring to scandals and corruption, mismanagement and misappropriation of public money during the applicant's term as Chief Executive Officer of the relevant public authority.[872] The applicant made seven claims to Google Inc. to remove eighteen links to the underlying reason that they were of severe effect to him. The applicant in the present case must be understood as a public person or a person having an important role in public life, for which the public interest is high, that the information in question was timely and concerned with professional public interest activity and also that their inaccuracies have not been proved; and thus the rejection of removal by Google Inc. was to be considered justified. Some links even referred to publications containing sensitive personal data regarding the prosecution of the applicant because of the defective recruitment of a close associate to him, that is to say sensitive data unrelated to the issue of public money laundering. Google Inc. rejected his request for the removal of the specific links related to his post as CEO, considering that the information in question concerned the applicant; was linked to his professional life and to his role as a person who plays a significant role in public life, and was not judged to be inaccurate or out of date and, as a result, its publication was of concern to the public. The Hellenic Authority for Data Protection, seeking to balance fundamental rights and interests and applying the common criteria at the European level in the present case, examined the justified or not of the negative response of Google Inc., i.e. a Google search engine operator.

To that end, the Authority first and foremost referred to the judgment in case C-131/12 of the CJEU ordering that the related European provisions; 'are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in

871 Explanatory Memorandum to the Law No. 4624/2019, page 27.
872 Decision No. 82/2016 of the Hellenic Authority for Data Protection.

fact satisfied, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful'.[873]

Following a balance between the right to privacy and the public's right to information and access to such information, the European Court had declared and the Hellenic Authority adopted the view that the relevant provisions; 'are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question'.[874]

In practice, however, as stated in the Guidelines issued by the Group of Article 29 of Directive 95/46/EC on the implementation of the judgment in case C-131/12, Google Spain (Opinion of WP 225, 26/11/2014), the impact of the prospect of deletion on individual Rights of Freedom to Expression and Access to Information will be very limited, as the authorities in the evaluation of the relevant cases about data protection should systematically take into account the interest of the public regarding access to information and, if the latter exceeds the rights of the data subject, this deletion would not be appropriate. As noted in this respect, the fundamental right to Freedom of Expression, within its meaning as 'Freedom to receive and impart information and ideas' in Article 11

873 The operative part (3) of the judgment in case C-131/12 of the CJEU.
874 The operative part (4) of the judgment in case C-131/12 of the CJEU.

of the EU Charter of fundamental rights must be taken into account when evaluating requests of data subjects.[875]

As regards the rights of the data subject, however, it should be noted that, given a publisher's abandonment of his blog and the inability of the data subject to the right to edit or delete his data, his position becomes difficult, even harmful. It should also be held that the appearance of the site, following a search by the Google search engine based on the applicant's name, significantly facilitates access to this inaccurate information and plays a key role in disseminating this information, and consequently constitutes a serious interference with the applicant's right to privacy. In the light of the foregoing, and in the light of the weighting of the conflicting rights and interests therein, it must be held that the applicant's request to Google Inc., as the controller, to remove the particular link must be satisfied, in particular except for the fact that the applicant is not a public person, by the nature of the information in question and its sensitive nature, the alleged inaccuracy of the above and the alleged damage to the subject.[876]

It should be noted that any search engine service provider, such as Google, is not required to initially review the content of the websites for which the relevant links are processed by the service, but only after a clearance request has been made to it.[877] However, once such a request is made to the entity - in which the request should provide with substantiated reasons for its submission - the entity should consider doing so by balancing the right to privacy and right of the public to accessing this information, taking into account also the legislation on the protection of personal data.[878] Moreover, according to the CJEU judgment C-131/12, that obligation applies even where the publication itself is legal.[879]

875 European Commission, Justice and fundamental rights, https://ec.europa.eu/justice/Article-29/documentation/opinion recommendation/files/2014/wp225_en.pdf accessed 30 July 2020.

876 Decision No. 83/2016 of the Hellenic Authority for Data Protection.

877 Opinion WP 225 of Working Party of the Article 29 states: 'The ruling does not necessarily apply to search engines for all information they process, but only when they have to respond to data subjects' requests for the exercise of their rights'.

878 Opinion WP 225 of the Working Party of the Article 29 states: '(…) search engines must comply with national laws for the protection of their requests and the content of their answers', as well as: 'In In order for the search engine to be able to perform the required assessment of all the circumstances of the case, data subjects must sufficiently explain the reasons why they request delisting, identify specific URLs and indicate whether they fulfil a role in public life, or not'.

879 Decision No. 25/2019 of the Hellenic Authority for Data Protection.

6. How does your country regulate the liability of internet intermediaries?

According to the Greek national legislation, the internet intermediaries enjoy, in principle, an immunity status. First and before all things, the Presidential Decree No. 131/2003 has transposed the Directive (EU) 2000/31 into the Greek legal order. Therefore, the Article 14 of the Presidential Decree No. 131/2003 provides that not a general liability of the service providers to control the information exists. In fact, the service providers do not hold such a general obligation to control the information transmitted or stored for the purpose of providing the services, nor hold they a general obligation to actively seek out facts or circumstances behind the information, which indicate that they refer to unlawful activities.[880] However, without prejudice to the provisions on the protection of privacy and personal data, the information society service providers are obliged to immediately inform the competent state authorities of any suspicion of unlawful information or activities being attempted by recipients of their services, and communicate to the competent authorities, at their request, any information facilitating the identification of recipients of their services with whom they have storage agreements.[881]

Under the specific circumstances, namely of the processes with regard to the cases of the simple transmission, cache storage, and hospitality of the information on the part of the internet intermediaries, a series of particular provisions apply.

The Simple transmission case: When an information society service is provided, consisting in the transmission of information provided by the recipient of the service to a communications network or in providing access to the communications network, the service provider shall not be responsible for the transmitted information, provided that the service provider: (a) is not the starting point for the transmission of the information; (b) does not select the recipient of the transmission; and (c) does not select or modify the information transmitted.[882] The transmission and access activities include the automatic, intermediate and temporary storage of the transmitted information, provided that the storage is for the sole purpose of transmitting to the communications network and does not exceed a reasonable time that is necessary for the transmission.[883] Nevertheless, the judicial or administrative authority always

880 Article 14, par. 1 of the Presidential Decree No. 131/2003.
881 Article 14, par. 2 of the Presidential Decree No. 131/2003.
882 Article 11, par. 1 of the Presidential Decree No. 131/2003.
883 Article 11, par. 2 of the Presidential Decree No. 131/2003.

keeps its jurisdiction to impose on the service provider the cessation or prevention of the alleged infringement.[884]

The Cache storage case: In the event of the provision of an information society service consisting of the transmission of the information provided by a recipient of service to a communications network, the service provider shall not be responsible for the automatic, intermediate and temporary storage of the information, which is for the sole purpose of making the subsequent transmission of the information to other recipients of the service more effective upon request, provided that the service provider: (a) does not modify the information; (b) complies with the conditions of access to information; (c) adheres to the rules for updating the information, which are widely recognised and used by the industry; (d) does not hinder the legitimate use of technology, which is widely recognised and used by the industry, in order to obtain data on the use of the information; and (e) acts promptly to retrieve the information stored or to make it impossible to access the information as soon as it realises that the information has been withdrawn from the network point where it was originally located or that the access to the information has become impossible or a judicial or administrative authority ordered the information to be withdrawn or denied access.[885] Nevertheless, the judicial or administrative authority always keeps its jurisdiction to impose on the service provider the cessation or prevention of the alleged infringement.[886]

The Hospitality case: When an information society service is provided consisting of storing the information provided by a recipient of the service, the service provider shall not be responsible for the information stored at the request of the recipient of the service, provided that: (a) the service provider does not really know that it is an illegal activity or information and that, and as far as any compensation claims are concerned, the service provider is not aware of the facts or circumstances resulting from the illegal activity or information; or (b) the service provider, as soon as it is aware of the above, rapidly withdraws the information or makes it impossible to access. However, the status of non-liability shall not apply when the recipient of the service is acting under the authority or control of the service provider.[887] The judicial or administrative authority always keeps its jurisdiction to impose on the service provider the cessation or prevention of the alleged infringement.[888]

884 Article 11, par. 3 of the Presidential Decree No. 131/2003.
885 Article 12, par. 1 of the Presidential Decree No. 131/2003.
886 Article 12, par. 2 of the Presidential Decree No. 131/2003.
887 Article 13, par. 1 of the Presidential Decree No. 131/2003.
888 Article 13, par. 2 of the Presidential Decree No. 131/2003.

Considering the legislative provisions highlighted above that attribute, under certain conditions, a general status of non-liability to the internet intermediaries, at the same time the national legal framework invokes for a *per legem genus* (i.e. under certain genus of the law) responsibility of the service providers in view of delimiting their enjoyed immunity;

From the Settings in the Electronic Communications concerning the Security and integrity of networks and services; taking the appropriate measures; All undertakings that provide for the public communications networks or publicly available electronic communications services shall take appropriate technical and organisational measures to properly manage the security of the networks and services. These measures, taking into account the latest technical possibilities, should ensure a level of safety commensurate with the existing risk. These businesses shall, in particular, take measures to prevent and minimise the impact of any security incidents affecting the users and the interconnected networks.[889]

From the settings concerning the Personal Data Protection; establishing an objective liability: According to the judgment of the CJEU in C-131/12, it was considered that the work of a search engine (in this case, Google Search of Google LLC), which displays search results in response to requests from Internet users searching for information about a person by its name, constitutes processing of personal data in the sense of Article 2 (2) (b) of Directive 95/46/EC (for GDPR, see Article 4 (2) respectively) and the search engine operator (in this case, Google LLC - formerly Google Inc.) is designated as the controller in the sense Article 2 (2) (d) of Directive 95/46/EC (for the GDPR, see Article 4 (7), respectively). This decision applies to search engine activity as a content provider, which consists of locating information published or posted online by third parties, automatically indexed, cached and ultimately made available to internet users in a certain preferable order, while such information includes personal dataAccording to par. 55 of the judgment of the CJEU in C-131/12: [890] 'In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable'.

889 Article 37, par. 1 of the Law No. 4070/2012.
890 Decision No. 25/2019 of the Hellenic Authority for Data Protection.

When the processing is carried out on behalf of a data controller, the latter shall ensure compliance with the obligations arising from the Law No. 4624/2019 that incorporated GDPR, and also with any other provisions concerning the protection of personal data. The right of the subject to update, correct, delete and limit the processing of his/her personal data, as well as to claim compensation in this case, shall be exercised against the controller.[891]

According to the Law No. 4624/2019, there are criminal sanctions provided on the absence of an authorisation on behalf of the subject of the data to the controller; Whoever, without right: a) intervenes in any way in a personal data archiving system, and by this act becomes aware of this data; b) copies, removes, alters, damages, collects, registers, organises, structures, stores, adapts, modifies, retrieves, searches for information, correlates, combines, restricts, deletes, destroys, is punishable by imprisonment of up to one (1) year, unless the act is more severely punished by another provision. Whoever uses, transmits, disseminates, communicates by transmission, has, announces or makes available to unauthorised persons' personal data, which he acquired, or allows unauthorised persons to become aware of such data, is punishable by imprisonment if the act is not more severely punished by another provision. If the act referred concerns specific categories of personal data referred to in Article 9 (1) of the GDPR or data relating to criminal convictions and offenses or related security measures referred to in Article 10 of the GDPR, the offender shall be punished by imprisonment of at least one (1) year and a fine of up to one hundred thousand (100,000) euros, if the act is not severely punished by another provision. The perpetrator of the acts referred to above shall be punished by imprisonment of up to ten (10) years, if he intended to offer himself or another illegal property benefit or to cause property damage to another or to harm another and the total benefit or total loss exceeds the amount of one hundred and twenty thousand (120,000) euros. If these actions endanger the free functioning of the democratic state or national security, imprisonment and a fine of up to three hundred thousand (300,000) euros shall be imposed.[892]

From the Criminal Settings of the Law; regarding the Intellectual Property rights: A person who without any right and in breach of the provisions of the law related to intellectual property rights, or the provisions of multilateral copyright international conventions, records works, reproduces them directly or indirectly, temporarily or permanently, in any form, in whole or in part, translates, adapts, or modifies them, distributes them to the public by sale or other means, or owns on purpose of their distribution, leases, publicly broadcasts, or broadcasts in any

891 Article 60, par. 1 of the Law No. 4624/2019.
892 Article 38, par. 1-5 of the Law No. 4624/2019.

other way, presents the works or their copies to the public in any way, imports copies of the work illegally produced abroad without the consent of the creator, and generally exploits works, copies of copyrighted works or infringes the moral right of the creator to decide on the work to be published and to present it to the public unaltered and without any additions or cuts, is punishable by imprisonment of at least one year and a fine of 2,900 EUR 15,000.[893]

From the Criminal Settings of the Law; regarding the unlawfulness of Minors Pornography: The general provision of the Greek Penal Code mentions that any person who is intentionally producing, distributing, publishing, displaying, importing or exporting from the national territory, transmitting, offering, selling or otherwise disposing of, purchasing, supplying, acquiring or possessing material relating to child pornography, or disseminating or transmitting information about perpetration of the above offenses, is punishable by imprisonment of at least one year and a fine.[894]

Besides, a distinct provision exists about Minors pornography crimes committed through information systems. In fact, the specific provision mentions that anyone who intentionally produces, offers, sells or otherwise disposes of, distributes, transmits, purchases, supplies or owns material relating to child pornography or disseminates information about the commission of the above acts through information systems, is punishable by imprisonment of at least two years, and fine.[895]

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1. Online content blocking and take-down

According to the national legislative framework, along with the enshrined concept of an 'Information constitution', which is in particular the established right of the individual to participate in the information society, there is also the judicial need to protect specific rights under national law, as for example intellectual property rights under Article 66E of the Law 2121/1993, where

893 Article 66, par. 1 of the Law No. 2121/1993. This Article has incorporated into national legal order the Article 8(1) of the Directive 2001/29. The Paragraph 1 of the Law No. 2121/1993 was replaced by paragraph 9 of Article 81 of the Law 3057/2002, Government Gazette A 239/10.10.2002.

894 Article 348A, par. 1 of the Law No. 4619/2019, (the recently introduced New Penal Code).

895 Article 348A, par. 2 of the Law No. 4619/2019, (the recently introduced New Penal Code).

online content blocking and take-down is explicitly permitted by the Commission for the Notification of Website Violations of Copyright and Related Rights. This certain Article has been officially introduced in Greek law with the Article 52, paragraph 1 of the latest Act 4481/2017. The comportment of the above-referred Commission sets out a very severe framework for future treatment of infringements online. If the Commission finds that the copyright or related right is infringed, it shall invite the recipients of the notice to remove the content infringing the right from the website to which it was posted illegally or to disable access to it. If the website on which the content is located is hosted on a server located within the Greek territory, the Commission invites the recipients of the notification to remove the specific content. In the event of large-scale infringements, the Commission may decide instead of removing the content to suspend access to it. If the website is hosted on a server outside the Greek territory, the Commission invites the Internet access provider to discontinue access to the content. In case of non-compliance with the operative part of the decision, the Commission shall impose a fine of five hundred (500) to one thousand (1,000) euros for each day of non-compliance. Among the criteria taken into account are the severity of the infection and its recurrence. According to the CJEU, the foregoing activity is permitted when there is an ad hoc court judgment declaring the content as illegal or the content in question is identical or slightly different from the content that had previously been judicially declared as illegal. It is up to the Member-States to incorporate in their national legal order the deemed as lawful – for the international standards- possibility of blocking and taking-down internet content. The national states are, therefore, granted a certain margin of discretionary power to decide towards the implementation of the restrictive measures in question. According to the ECHR, there is also a wide margin of appreciation left to the states to strike a weighing balance of the competing rights, taking into consideration the overriding 'necessity' of the measure regarding blocking or/and taking-down 'in a democratic society'. Subjective criteria, like 'having been aware of the illegal content' can also be taken into consideration as under the case of the hospitality of the provider predicted in Directive (EU) 2000/31 and subsequently in Presidential Decree 131/2003. So, taking all the tensions into account, it seems that the national legislation is expected to gradually comply with the EU and international standards, i.e. it shall develop in the next five years towards the crystallisation of the proportionality rule in all the main legal provisions to ensure legal certainty and alignment with the settled European principles.

7.2. The liability of internet intermediaries

According to the national settled case law, the service provider's immunity is predominant and there exists not an obligation on the part of the service providers to general control. In fact, the host company (website) cannot, in principle, be considered as the owner of the blog content by an analogy application of the press legislation. On the contrary, it is feasible from the press legislation to establish a duty to detect illegal content, as the service provider is the owner of the means of the moving information or news, addressing a large number of internet users on the purpose of their updating. The analogical application of the press legislation inserts an objective basis for the civil liability of the internet intermediaries to be grounded. According to the CJEU, the national courts have a jurisdiction to impose measures to bring an end to an infringement, but also to prevent it. In view of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, and in order to achieve a well-functioning and fair marketplace for copyright,[896] it is recommended at the European Union level to have a harmonised legal protection for press publications in respect of the use of protected content by online content-sharing service providers. Such protection should be effectively guaranteed through rights related to copyright for the reproduction and making available to the public of press publications of publishers established in a Member State in respect of online uses by information society service providers within the meaning of Directive (EU) 2015/1535 of the European Parliament and of the Council.[897] According to Article 29 of the Directive (EU) 2019/790, Greece, among other Member States of the European Union, shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 7 June 2021. Thus, Greece is supposed by then to communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive and in line with it. According to the above, latest (see EU Dir. 2019) perceived outline for the liability of internet intermediaries, an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of the Directive (EU) 2019/790 when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users. All Member States – Greece included – are

[896] Recital 3 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[897] ibid, recital 55.

invited to provide that a service provider shall obtain an authorisation from the right holders referred to in Article 3(1) and (2) of Directive 2001/29/EC, for instance by concluding a licensing agreement.[898] Therefore, when an online content-sharing service provider performs an act of communication to the public or an act of making available to the public under the conditions laid down in the Directive in question, the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article, except for purposes falling outside the scope of Directive (EU) 2019/790 where the so-called immunity status remains.[899] Thus, the service providers which perform an act of online content-sharing where no authorisation is granted, shall be liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter, unless the service providers demonstrate that they have: a) made best efforts to obtain an authorisation, and b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided the service providers with the relevant and necessary information; and in any event c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightsholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads.[900] In determining whether the service provider has complied with its obligations, and in light of the principle of proportionality, the following elements, among others, shall be taken into account: a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and b) the availability of suitable and effective means and their cost for service providers.[901] Greece among all Members States, shall provide that, in respect of new online content-sharing service providers the services of which have been available to the public in the Union for less than three years and which have an annual turnover below EUR 10 million, calculated in accordance with Commission Recommendation 2003/361/EC, the conditions under the liability regime are limited to make best efforts to obtain an authorisation and to acting expeditiously, upon receiving a sufficiently substantiated notice, to disable access to the notified works or other subject matter or to remove those works or other subject matter from their websites. Where the average number of monthly unique visitors of such service providers exceeds 5 million, calculated on the

898 ibid, Article 17, par. 1-2.
899 ibid, Article 17, par. 3.
900 ibid, Article 17, par. 4.
901 ibid, Article 17, par. 5.

basis of the previous calendar year, they shall also demonstrate that they have made best efforts to prevent further uploads of the notified works and other subject matter for which the rightsholders have provided relevant and necessary information.[902] It is worth to mention that the application of Article 17 of the Directive (EU) 2019/790 shall not lead to any general monitoring obligation.[903] Besides, Greece is expected among other Member States to provide that online content-sharing service providers put in place an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them. Member States shall also ensure that out-of-court redress mechanisms are available for the settlement of disputes, but also that users have access to a court or another relevant judicial authority to assert the use of an exception or limitation to copyright and related rights. In any case, online content-sharing service providers shall inform their users in their terms and conditions that they can use works and other subject matter under exceptions or limitations to copyright and related rights provided for in Union law.[904] As regards the compensation liability in case of copyright infringement, there is an arising need for the harmonisation of certain aspects of copyright and related rights in the information society, read in conjunction with the European legislation on the enforcement of intellectual property rights. It must be borne in mind, first, that, according to the CJEU's case law, EU law requires that, when transposing directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the EU legal order. Subsequently, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of EU law (judgment of 16 July 2015, *Coty Germany*, C-580/13, EU:C:2015:485, paragraph 34).[905]It should be noted that Article 52(1) of the Charter[906] states, inter alia, that any limitation on

902 ibid, Article 17, par. 6.

903 ibid, Article 17, par. 8.

904 ibid, Article 17, par. 9.

905 CJEU, judgment of 18 October 2018, *BasteiLübbe GmbH & Co. KG v Michael Strotzer*, Case C-149/17, ECLI:EU:C:2018:841, par. 45.

906 Article 52, par.1 of the Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 'Scope of guaranteed rights; Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'.

the exercise of the copyright protection as well as all the rights and freedoms recognised by the Charter must respect the essence of those rights and freedoms and that it is apparent from the case law of the European Court that a measure by service providers, which results in serious infringement of a right protected by the Charter is to be regarded as not respecting the requirement that such a fair balance be struck between the fundamental rights which must be reconciled (judgment of 16 July 2015, Coty Germany, C-580/13, EU:C:2015:485, paragraph 35).[907]

7.3. The right to be forgotten

According to the national settled case law, there is a list of nationally shared criteria that should be taken into consideration in the weighing process of the competing rights. An illegal processing of sensitive personal data happens without a strong public interest for the publication of the data to have been previously declared. According to the CJEU, the right to erase one's personal data does not pre-suppose a prejudice attributable to the data subject. The right of the individual to be forgotten overrides not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information. However, this is not the case if the interest of the general public is deemed preponderant. According to the ECHR, the concept of an individual's 'informational self-determination' deserves judicial protection. A substantial contribution of the Internet exists as the latter is an important source for education and historical research due to its accessible and free character. The risk of harm posed by content and communications on the Internet is certainly higher than that posed by the press. Any measures of compliance and the measurement of interference with Freedom of Expression lie in the discretionary area defined as the national margin of appreciation on the part of the state. The European supervision ensures that the principles derived from ECHR's case law guide the state's assessment. So, taking all the tensions into account, it seems that the national legislation is expected to gradually comply with the EU and international standards that put an emphasis on the protection of the human integrity, i.e. it shall develop in the next five years towards highlighting the potential harm caused to the individuals by the spread of their personal data through the Internet and towards imposing a limitative legislative framework to restrict the cases that the public is predominantly entitled to have access to personal sensitive information.

---

907 CJEU, judgment of 18 October 2018, *BasteiLübbe GmbH & Co. KG v Michael Strotzer*, Case C-149/17, ECLI:EU:C:2018:841, par. 46.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

8.1 What is hate speech?

Although there is no predetermined definition of 'hate speech', it is widely accepted that hate speech is an expression of discriminatory hate towards people. This broad definition of hate speech captures a very broad range of expression, entailing even lawful expression.[908] According to the European Court of Human Rights, in a definition adopted by the Council of Europe's Committee of Ministers, 'hate speech' envisages: 'all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility towards minorities, migrants and people of immigrant origin.'[909] Many institutions have given a definition of hate speech, however the problem is this exact lack of a universally accepted definition.[910] Article 19 of the ICCPR[911] considers that grounds for protection against 'hate speech' should include all those characteristics which appear under the broader non-discrimination provisions of international human rights law. However, this is not how hate speech is confronted in practice. This is due to the fact that no country wants to provide for certain definitions and content of hate speech, for fear of narrowing down the right of Freedom of Expression.[912]

For the better understanding of what hate speech entails, a typology has been constructed. Under this typology, there is; (i) prohibited hate speech, according to Article 20(2) of the ICCPR, (ii) 'hate speech that may be prohibited', which can be prohibited by the States if the forms of hate speech comply with Article 19(3) of the ICCPR, (iii) lawful hate speech, which although discriminatory, can be protected from restrictions under Article 19(2) of the ICCPR.[913]

---

908 'Hate Speech' Explained, (2015), page 10.

909 Recommendation No. R(97)20 of the Council of Europe Committee of Ministers on 'Hate Speech,' 30 October 1997.

910 'Hate Speech' Explained, (2015), page13.

911 International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

912 Hate Speech Explained, (2015), page 14.

913 UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) in his annual report to the General Assembly, A/76/357, 7 September 2012, 'Hate Speech' Explained, (2015), page 13.

It is true that we live in an era of mal-communication, especially now that the Internet and the various social media open the room for the unfiltered expression of everyone's opinions and ideas. Instances of dis-information, mal-information and mis-information are all flourishing throughout the net and on social media.[914] When journalists, political lobbies and the private sector try to profit through this expansion of hate speech on the net, things get more perplexed. Do social media owners and news companies really want and can protect users and individuals from hate speech?

8.2 International & European law concerning the Greek law order on hate speech & Freedom of Expression

Article 10 of the Convention on Human Rights orders that everyone has the right to Freedom of Expression. In particular, the right includes the freedom to hold and receive information and ideas without interference, therefore establishing two distinct elements of Freedom of Expression. According to Section 10(2) of the same Convention, the exercise of this freedom may be subject to formalities, conditions, restrictions or penalties that are prescribed by law and are necessary in a democratic society. These limitations are enacted for the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for the prevention of the disclosure of information received in confidence, for the maintenance of the impartiality of the judiciary.[915]

Freedom of Expression, as protected by Article 10 paragraph 1 constitutes an essential basis of a democratic society and limitations on that freedom foreseen in Article 10 paragraph 2 are interpreted strictly.[916] In the judgment Editorial Board of *PravoyeDelo and Shtekel v. Ukraine*, (no. 33014/05, 5 May 2011), the Court acknowledged that Article 10 of the Convention had to be interpreted as imposing on States a positive obligation to create a statutory framework to ensure effective protection of Freedom of Expression on the Internet.[917]

However, hate speech does not benefit from the protection of Article 10 of the Convention.[918] This was eloquently stated in the case *Gündüz v. Turkey*, no.

---

914 Dis-information; Information that is false and deliberately created to harm a person, social group, organization or country, Mis-information; Information that is false, but not created with the intention of causing harm, Mal-information; Information that is based on reality, used to inflict harm on a person, organization or country. According to Claire Wardle, Hossein Derakhshan, Information Disorder; Toward an interdisciplinary framework for research and policymaking, (27 September 2017), page 20.

915 Article 10(1),10(2) of the ECHR.

916 Internet: case law of the European Court of Human Rights, June 2015, page 17.

917 ibid, page18.

918 Internet: case law of the European Court of Human Rights, June 2015, page19.

35071/97*,* where a member of an Islamist sect, in his appearance in a television show, criticised democracy and called for the application of Sharia Law. A prosecution was then enforced against him, on the grounds that his words were considered speech that called for violence and religious intolerance. The Court considered that, given that Mr Gündüz's words were expressed in a public debate and given that the debate itself wanted to present the unorthodox opinions and ideas, beforehand incompatible with democratic principles, the speech of this man was not regarded as 'call to violence' or 'hate speech'. A dissenting opinion was also formed, however, stating that indeed Mr Gündüz's speech was hate speech and had cultural implications.[919]

Freedom of Expression protected by Article 10(2) also covers information or ideas that offend, shock or disturb the State or any section of the population.[920] Therefore, criticism and satire, even irreverent satire are covered by the Convention. The justification to this is that they serve for the promotion of pluralism, tolerance and broadmindedness, which are inherent in a democratic society. However, offensive and injurious speech on the Internet that goes beyond the satirical and defamatory register, leads the Court to reject an application.[921]

Regarding journalism, the case *Kącki v. Poland*, has to offer useful guidance. The case concerned a telephone interview, taken by a Polish journalist about a 'sex scandal', which had become very widely known in the polish district. The journalist had then publicised the interview, due to which criminal proceedings were initiated against him. The Court found that the domestic court had not undertaken the balancing test that requires a balancing exercise of the competing interests at stake. Lastly, the Court reiterated that the nature and severity of the penalty imposed are factors to be taken into account when assessing the proportionality of the interference, explaining that the initiation of criminal prosecution against the journalist was a disproportionate measure and therefore resulted in a violation of Article 10 of the Convention.[922]

Under international law, there are forms of hate speech that must be prohibited by States, according to the typology of hate speech presented above. First of all, prohibited hate speech entails 'direct and public incitement to genocide, prohibited in the Convention on the Prevention and Punishment of the Crime

919 *Gündüz v. Turkey*, no. 35071/97, <https://globalfreedomofexpression.columbia.edu/cases/gunduz-v-turkey/ accessed 30 July 2020..

920 Kącki v. Poland, par.42.

921 Internet: case law of the European Court of Human Rights, June 2015, page 20.

922 *Kącki v. Poland*, para. 56-57.

of Genocide[923](1948) and the Rome Statute of the International Criminal Court[924] (1998), as well as the war crime of persecution. Second, any advocacy of discriminatory hatred that constitutes incitement to discrimination, hostility or violence, as analogous to Article 20(2) of the ICCPR. Third, according to Article 4 of the International Convention on the Elimination of all Forms of Racial Discrimination (the ICERD) 'all propaganda and all organisations which are based on ideas of theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in [the UDHR] and the rights expressly set forth in Article 5 of [the ICERD]' are condemned.[925] There is also the Committee on the Elimination of Racial Discrimination, which adopted General Recommendation No. 35 on 'combating racist hate speech'. The Recommendation includes in general the definition of hate speech as regarded in contrast to the Freedom of Expression.[926]

According to the typology of hate speech above, there is also hate speech that 'may be prohibited'. According to Article 19(3) of the ICCPR, there is a three-tier test that must be satisfied.

(i) The restrictions must be provided for by law, (ii) in pursuit of a legitimate aim, such as respect for the rights of others, and, (iii) the restrictions must be necessary in a democratic society.[927]Forms of hate speech that individually target an identifiable victim do not fit within the criteria of Article 20(2) of the ICCPR.[928]

Third, there is also the form of lawful 'hate speech'. In this regard, the speech does not meet the threshold of severity described above. However, this does not preclude States from taking legal and policy measures to fight 'hate speech'.[929]

Proceeding to the analysis of elements (i) - (iii) above, as envisaged in Article 19(3) of the ICCPR, states should combat hate speech using laws, measures and

---

923 The Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948, UN Treaty Series, vol. 78, page 277, Article 3(c).

924 The Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998, Article 6, Article 25(3)(e).

925 International Convention on the Elimination of All Forms of Racial Discrimination, 21 December 1965, UN Treaty Series, vol. 660, page 195.

926 ICERD Committee, CERD/C/GC/35, 9 September 2013.

927 Article 19(3) of the ICCPR.

928 Article 20(2) only envisages cases of incitement of hatred ('2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.')

929 'Hate Speech' Explained, (2015), page 20-22.

regulations, that are provided by law, meaning that they must be precise and concrete in their wording, so as to enable individuals to act accordingly (i), in the pursuit of a legitimate aim, so as to say, for the respect of the rights of others, or the protection of national security or public order, or of public health or public morals (ii) and the measures enforced must be necessary in a democratic society, in other words, assuring that there is a sufficient nexus between the expression in question and the threat imposed for the protection of such rights as explained under (ii), providing for the necessity and proportionality of the specific measure (iii).[930]

It is true that multilateral action is the only effective and workable legal tool that can be used to obviate the development and expansion of hate speech online. The Council of Europe's Convention on Cybercrime is the first multilateral effort for the tackling of computer based crime, containing regulations for illegal access (Article 2), illegal interception (Article 3), and content-related offences,[931] thus reinforcing international cooperation and the harmonisation of national laws throughout the various law orders.[932] A separate Protocol to the Convention was also enforced, to address hate speech online. This Protocol requires of the Parties to criminalise racist and xenophobic behaviour conducted through computer systems. [933] There are five types of conduct that Parties are required to criminalise; (1) 'distributing or otherwise making available, racist and xenophobic material to the public through a computer system', (2) the act of directing a threat to a person through the Internet purely because of race, national origin, or religion, of which parties cannot opt out, (3) the act of publicly insulting a person through a computer system because of the person's race, national origin, or religion, (4) the distribution or the availability in the Internet of 'material which denies, grossly minimises approves or justifies acts constituting genocide or crimes against humanity.', and (5) the 'aiding or abetting' of the commission of any of the offenses established by the Protocol.[934]

Lastly, the right to Freedom of Expression is also founded on the Charter of Fundamental Rights of the European Union, where it is explicitly stated on Article 11; 'Everyone has the right to Freedom of Expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.', while

930 ibid, page 67.
931 Convention on Cybercrime (ETS no. 185).
932 Banks J., 'Regulating Hate Speech Online', (2010), International Review of Law, Computers & Technology Vol. 24, No. 3, 233- 239, page236.
933 ibid.
934 Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Emerging American Haven', (2005), page792-794.

on Article 21 discrimination of all kinds is condemned 'on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'.[935]

8.3 The level of protection against hate speech in the Greek law

All the above is very important for the definition of hate speech and the adoption of a typology that can confront all kinds of hate speech, however what is of the utmost importance is to which extent the supranational laws and conventions are integrated in the Greek law order. Greece has ratified the International Covenant for Civil and Political Rights (ICCPR), by means of the Presidential Decree 2462/1997, thus conforming with the provisions against hate speech analysed above, under Article 19(3) and Article 20(2).By reason of Article 28(1) and only after the Revision of the Constitution of 1975, the provision of Article 10 of the ECHR, as well as the provisions of the CFREU, became an integral part of the Greek law.[936]

The Freedom of Expression is founded in the Greek Constitution in Article 5(1) as well as Article 14(1). According to these Articles, 'everybody has the right to freely develop their personality and participate at the social, economic and political life of the Country, given that they do not infringe the rights of others or the Constitution or public morals'[937] while under Article14(1), 'everybody has the right to express and disseminate orally, in written form and through the press their opinions in accordance with the laws of the State'. [938]The enumeration of means of expression in Article 14(1) is not exhaustive, therefore the Internet is also considered a means of expression protected by the Article.[939] Under the Greek Constitutional Law, however, Freedom of Expression must be exercised 'in accordance with the laws of the State'.[940] Therefore, only with due regard to laws and regulations of the State is the right of Freedom of Expression to be exercised.

Apart from the provisions in our Constitution, the greatest step towards fighting discrimination was the enforcement of a special law, in 2014. The most

935 Articles 11§1, 21§1 of the Charter of Fundamental Rights of the European Union.

936 G. Stavropoulos, 'The influence of ECHR on the Greek law order' <https://www.constitutionalism.gr/stavropoulos-esda-elliniki-ennomi-taxi/> accessed at 30 July 2020.

937 Article 5(1) of the Greek Constitution.

938 Karakostas I.,(2009), Law & the Internet, page41, Thesis of Papas I, 'The protection of personality in the net', (2011), page 26, <https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1322688/theFile/1322689>.

939 Manual of Constitutional Law, Pantelis A., (2016), page 504, par. 493.

940 Article 14(1) of the Greek Constitution.

significant and systematic amendment of the anti-racism legislation in Greece is the Law 4285/2014 'Modification of the Law No. 927/1979 and adjustment to the Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, and other provisions', modernised the national legislation against racial phenomena in fulfilment of the European legislation.

According to the provisions of the Law No. 4285/2014 (Article 10) 'antiracism Law', Article 81A 'racist crime' was added in the Greek Criminal Code (hereon grCC) introducing the autonomous punishment of racial motivation. Since 2008, the element of racial motivation was generally taken into consideration in the terms of the judicial determination of the penalty in the Article 79 grCC.

Specifically, Article 81A provided for stricter sentencing frame, namely, aggravating the lowest penalty that could be imposed for hate motivated crimes due to the racial, national or ethnic origin, colour, religion, sexual orientation, gender identity or disability of the victim. The prohibition of suspending the case remained also in Article 81A grCC. Afterwards, Article 21 of the Law No. 4356/2015 amended the Article 81A by providing for also stricter maximum penalty in cases of misdemeanours, abolishing the prohibition of suspending the sentence, and also abolishing hatred as a necessary *mens rea* element.[941] More recently, Law 4619/2019, amended the Criminal Code, providing for a different treatment of the 'racist crime'. Namely, Law 4619/2019, any kind of racial motivation in the commitment of a crime is punished with imprisonment of up to one year in the case of a misdemeanour and with a least of two years in the case of a crime. What can be spotted is a decrease of the maximum penalty limits, which can be probably interpreted as a sign of deprecation of the 'racist crime', as a special kind of crime. This new regulatory framework could maybe signify an attempt to disempower its importance in the Greek legislation, although great effort has been taken to combat hate speech and any kind of hate rhetoric with many other provisions in the Criminal Code.

Especially, the Greek Criminal Code provides for crimes that are conducted through the Internet. According to Article 183 of the grCC, 'whoever [...] through the Internet incites or provokes defiance against the laws or the decrees or other legal orders of the Authorities, is punished with up to one year of prison or with a penalty fee'. The same sentence is provided for the incitement to commit a misdemeanour or crime, thereby exposing public order to danger.[942] A more eloquent provision for the protection against hate speech is the

941 Pitsela, Chatzispyrou, (2017), page1536, 1537.
942 Article 184(1) of the Criminal Code.

commitment of the crime of Article 184(2) of the Criminal Code. According to it, an up-to-three-year sentence or a penalty fee is imposed on the perpetrator of the crime of Article 184(1), if through the commitment of the crime of Article 184(1), the execution of violent acts against a group or an individual is attempted, based on their race, colour, national origin, genealogical factors, their religion, disability, sexual orientation, identity or sex.[943] The same follows for Article 187A grCC, where 'whoever publicly through the Internet incites or provokes the commitment of a terrorist act, exposing public order to danger, is punished with imprisonment.' Under the Greek Criminal Code, an infringement of Article 14(1) of the Constitution can result in the commitment of the crimes against Honour, as provided by Articles 361 etc. of the Criminal Code. These Articles envisage the crimes against reputation, including verbal abuse and defamation.[944]

To this regard, the Greek law order has taken great steps towards the positive regulation against hate speech through the Internet. Indeed, after the amendment of the Criminal Code with the recent law 4619/2019, an express provision for the commitment of the related crimes online is added, a regulation which was not included in the previous Criminal Code.[945] This development may be leading us to a double-edged sword; on the one hand, our national law order takes steps towards the incrimination of clearly unlawful behaviours, such as terrorist attacks of Article 187A, crimes against public order (Articles 183, 184 of the Criminal Code), in accordance with the guidance provided to it by the definitions of 'hate speech' included in the ECHR and the ICCPR.

However, maybe this over-regulation providing for the commitment of crimes via the Internet testimonies an indirect contravention of States' obligation to safeguard Freedom of Expression online, especially when the issue of new laws specifically designed to criminalise expression on the Internet comes to light. [946] According to the Special Rapporteur, defamation should be decriminalised, and protection of national security or countering terrorism can only be justified if; (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.[947]

---

943 Article 184(2) of the Criminal Code.

944 Wolfgang Benedek and Matthias C. Kettemann, Freedom of Expression and the Internet, page 82.

945 e.g. the previous Article for defamation (Article362 of the Criminal Code), provided for as follows; 'Whoever by any means in front of a third party asserts or disseminates for somebody else a fact that can injure their honour or reputation is sentenced to imprisonment [...]. However, under the revised Criminal Code, an express addition is made; 'If the act has been committed publicly by any means or through the Internet, imprisonment is imposed.'

946 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc.A/HRC/17/27, La Rue F. (16 May 2011), para. 34.

947 ibid, para. 36.

Notwithstanding the aforementioned, the Greek Constitution already provides for a four-prong test in order for the online expression to be restricted; (i) the opinion expressed must be of public interest, (ii) refer to a public figure (iii) the existence of *bona fide* with regard to the content expressed, (iv) aim of the expression must be the exercise of criticism and not the defamation of another person. This happens because, in general, the Greek Constitution avoids a chilling effect on the Freedom of Expression and stands for pluralism and the promotion of Freedom of Expression.

This is also evident from the fact that Internet intermediaries and Internet servers are not held responsible for the information provided on the Internet at sites and blogs, under certain conditions[948],according to the Presidential Decree 131/2003, which ratified Directive 31/2000/EU.[949] The takedown of posts by the relevant Internet server, as provided for in Article 14(5) of the Greek Constitution[950] cannot be considered to diminish Freedom of Expression online. Article 14(5) provides for the right of reply for anyone insulted by an imprecise or insulting or defamatory post or emission, while the server has the obligation of '*complete and immediate restitution*'.[951] This constitutional guarantee, as far it is not subject to abuse by States, can provide for a satisfactory regulating content. However, Internet intermediaries must be handed the resources to challenge such takedowns, since the uncontrolled 'notice-and-takedown' mechanism can result in over-censoring in websites by Internet servers.[952]

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

The Greek Constitution is placed in favour of the promotion of Freedom of Expression online, through the provisions of the Greek Constitution analysed above. A chilling effect on Freedom of Expression online is not at all compatible

948 Article 12(1) ('Mere Conduit') of Directive 31/2000/EU; 'Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: a) does not initiate the transmission; (b) does not select the receiver of the transmission; and c) does not select or modify the information contained in the transmission.', Vlachopoulos S., (2017), Fundamental Rights, page 299.

949 Vlachopoulos S., (2017), Fundamental Rights, page 294-300.

950 Manual of Constitutional Law, Pantelis A., (2016), page 502, para. 491.

951 Article 14(5) of the Greek Constitution.

952 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/17/27, La Rue F. (16 May 2011), para. 42.

with the will of the Greek legislator. This is the reason that any insulting or defamatory content contravening the Constitution or the Criminal Code is examined thoroughly, with due respect to the principle of proportionality (as envisaged in Article 25 of the Greek Constitution) and with accordance to the guidance provided by the ECHR and the ICCPR, in order for an *in concreto* finding of an infringement, surpassing the limits set in the Constitution.[953] However, the right to Freedom of Expression online can be in conflict with other fundamental rights.[954]

9.1. The Freedom of Expression and its interconnection with other rights

In particular, the right to Freedom of Expression online can be found to contravene; the right to information (Article 5A of the Constitution) (a), privacy and the right to personality (Article 57 of the Civil Code and Article 9A and 19 of the Constitution) with regard to the issue of anonymity in the net (b), the IP (Intellectual Property) rights, as envisaged in Article 17 of the Constitution (c),[955] and the protection of childhood in the net (d). The distinct elements (a) to (d) will be further addressed below.

9.1.1. Freedom of Expression and the right to information

According to Article 5A (1) of the Greek Constitution, 'All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties.', while according to the second paragraph of the same Article, 'All persons have the right to participate in the Information Society.' The provision of paragraph 1, also provides for the protection of the right to information, provided it is not conducted in such a way that it exposes the State or the rights of others to danger. As provided by the European Human Rights Court in K.*U. v. Finland* 'Although Freedom of Expression [...] and confidentiality of communications are primary considerations [...] , such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.' [956] The problem posed here is the achievement of the right equilibrium between the Freedom of Expression and the right of people to get informed, disseminate and diffuse information on the one hand and the legitimate restriction of such rights due to the infringement of other

953 Vlachopoulos S., (2017), Fundamental Rights, page 290, para. 25.
954 ibid, pp. 296-297.
955 ibid, page 296, 297.
956 Internet: case law of the European Court of Human Rights, June 2015, page24.

rights (such as the right to privacy), when the diffusion and publication of information and opinions on the net is exercised beyond the limits provided by Article 5A, in accordance with the principle of proportionality of Article 25.[957] [958]

9.1.2. Freedom of Expression and the respect of privacy - safeguard of anonymity

According to Article 9A of the Constitution, 'All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law.' According to Article 57 of the Civil Code, introducing the right to personality, the protection of one's personality is a general clause, the content of which is examined *in concreto* according to the relevant laws and case law. The right to personality is personal, absolute and inalienable.[959] The information provided by Article 9A, namely the personal data, are indispensable part of the right to one's personality, since everybody has the absolute right to manage and publicise their personal information to the people that they desire to, for the aims and goals that the persons think this information serves for. Therefore, the personal data protected in Article 5A form an integral part of everyone's right to personality, as envisaged in Article 57 of the Civil Code.[960] The protection of personal data and one's personality against the Freedom of Expression must again be struck after the evaluation of Article 25 of the Constitution and the balancing between such rights so as to distinguish which right deserves and ought to be protected. The aforementioned principle of proportionality consists in a three-prong test that assesses (a) whether a measure that interferes with a right is suitable for achieving its objective, (b) whether it is necessary for that purpose, and (c) whether it burdens the individual excessively compared with the benefits it aims to secure.[961]

In the field of the Greek law, two relevant cases can be mentioned, namely 65/2004 of the first Instance Court of Athens and 9099/2005 of the Appellate Court of Athens, pertaining to the unlicensed publication of personal letters of

---

957 Article 25(1) provides as follows; 'Restrictions of any kind which, according to the Constitution, may be imposed upon these rights, should be provided either directly by the Constitution or by statute, should a reservation exist in the latter's favour, and should respect the principle of proportionality.'

958 Vlachopoulos S., (2017), Fundamental Rights, page 303, para. 54.

959 Article 57 of the Greek Civil Code.

960 Thesis of Papas I., 'The protection of personality in the net', (2011), page 37 and 38 <https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1322688/theFile/1322689> accessed 30 July 2020.

961 Tsakyrakis S., 'Proportionality: An assault on human rights?' <https://academic.oup.com/icon/Article/7/3/468/703178> accessed 28 February 2020.

some renown politicians' relatives. The first instance Court ruled that there was public interest that justified the publication of such content, given the relation with the known political figures, however, the Appellate Court overruled the decision of the first instance Court and judged to the contrast that 'the relation of a person with persons of topicality, such as the persons of public political life, can incite the interest of journalists, however, it cannot encroach on another's right to personality and self-determination.'[962] This case pertains to another dimension of the protection of privacy, namely, the protection of secrecy of letters and all other forms of free correspondence, including electronic correspondence.[963]

This case is really enlightening for incidents that pertain to publications of journalists and have to do, in their majority, with persons and situations of public interest. This is one side of the coin. Another really important issue, however, is the regulation of privacy and Freedom of Expression, with regard to the countless anonymous users of the net, who continually share, comment, impart and react to the content included, at the various websites, blogs, sites and social media. A certain problem that arises is the protection of anonymity and whistle-blowing on the Internet, while addressing illegal speech on the net.[964] It is true that by the present operation of sites, blogs and social media, anybody can easily post and share ideas and opinions likely to infringe the limits of legitimate freedom of expression without being traced. Social media operators and blog owners would not opt to limit one's anonymity on the net, since this could have devastating results for their financial interest.[965]

At the same time, whistle blowers must use appropriate means to achieve their aims. Their role is to be able to divulge facts likely to interest the public and contribute to transparency in the dealings of representatives of the public authorities. They must conduct their affairs 'with the necessary vigilance and moderation'. However, whistleblowers are not at all entitled to insult or make known to the public other people's right to privacy and personality, with respect to their reputation. Nor do the rights of whistleblowers extend to the publication of false or deformed information. The domestic courts have the power to 'weigh' the case on occasion and evaluate the impact of the statements made, with regard

962 Vlachopoulos S., (2017), Fundamental Rights, page 300-301, para. 48, ΠΠΡΑθ 65/2004, ΕφΑθ 9099/2005.

963 Article 19(1) of the Greek Constitution provides as follows; 'Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable.'

964 Wolfgang Benedek and Matthias C. Kettemann, Freedom of Expression and the Internet, page 37.

965 Protalinski E. (15 November 2011), 'Facebook name battle: Ahmed Salman Rushdie claims victory', www.zdnet.com/blog/facebook/facebook-name-battle-ahmed-salman-rushdie- claims-victory/5358.

to all the interests at issue.[966] At any cost, an outright prohibition of whistle-blowing would unnecessarily restrict Freedom of Expression online. For example, in *Guja v. Moldova* (GC), the Court found that the disclosure of confidential information by a civil servant denouncing illegal conduct or wrongdoing at the workplace was protected by Article 10, because of the strong public interest involved.[967] Therefore, again, an enforcement of the Greek Constitution Article's 25 evaluation test is needed, in order to compare and weigh the conflicting interests of the public, the protection of one's privacy and the unlawfulness of the whistleblowers' publication.

The recent law 4624/2019 provides for a more specific regulatory framework towards the protection of personal data, thus in an attempt to incorporate the Regulation 2016/679/EU and modernise the protection of the users' privacy. Article 28 of the aforementioned law provides for some specific conditions in order for the process of personal data, amid which the subject of the personal data must provide its consent for such process, as well as with the condition that the right to information and the right to Freedom of Expression overrides the right to the protection of personal data.[968] The incorporation of the European legislation in the Greek law order testimonies an attempt for unanimous protection of the personal data of Internet users with due consideration for the right to Freedom of Expression.

9.1.3. Freedom of Expression and IP rights

The Internet is prominently used for uploading, sharing and the reproduction of any kind of intellectual endeavours, from scientific Articles to songs, music and Article The access to some of this work cannot be obtained without some kind of registration, subscription or other forms of protection of the IP right of the creator.[969] Article 17(2) of the Greek Constitution provides as follows 'No one shall be deprived of his property except for public benefit which must be duly proven'. According to Article 1(1) of law 2121/1993, the creators of such creations acquire intellectual property, which includes exclusive and absolute rights, the right to use and dispose of their creation (property right) and the right to protect their personal connection to it (moral right). Expressly, Article 2 of the same law, the databases which fulfil the requirements, are also considered protected intellectual property under the Greek law.[970] However, this particular

966 Internet: case law of the European Court of Human Rights, June 2015, page 26.
967 Wolfgang Benedek and Matthias C. Kettemann, Freedom of Expression and the Internet, page 38.
968 Article 28§ 1, Law 4624/2019, <https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4624-2019/arthro-28-nomos-4624-2019-epexergasia-kai-eleytheria> accessed 30 July 2020.
969 Vlachopoulos S., (2017), Fundamental Rights, page 297.
970 Article 2(2a) of the Greek law 2121/1993.

law provides for a differentiation; the protection of IP rights that derive from the construction of an electronic database does not offend no other right that exists in the context of the database.[971]

9.1.4. Freedom of expression and the protection of childhood

Freedom of Expression encompasses the right to impart ideas that may be unsuitable for some age groups, such as offensive information.[972] According to the European Court of Human Rights, a balance must be always struck between the harmful content and the protection of childhood. Individuals of young age are vulnerable and must be treated carefully. According to Article 21 of the Greek Constitution, in accordance with the guidance provided by the Court, 'childhood shall be under the protection of State'.[973]

Concerning case law, in *K.U. v. Finland*, an unknown person had published the personal details of a twelve-year-old on a dating website. This obviously put the child in danger of sex predators. Missing any law for 'notice-and-takedown' of information in the Finnish law order, the privacy of the child had been infringed. Given that anonymity places a certain burden on States to trace down victims of privacy violations, especially in case that they affect the protection of childhood, states have to provide a legal framework sufficient to pierce the veil of anonymity in serious cases. Safeguards might include precautionary measures by social networks, including filtering for keywords, but must at least include ex post moderation of content flagged as inappropriate for young users.[974]

The only safeguard for child abuse and child pornography is envisaged at Article 348A paragraph 2 grCC, as it was initiated by Law 4267/2014 'against child abuse and exploitation and child pornography'. According to this Article, 'Whoever intentionally produces, offers, sells or in any way has, distributes, transmits, purchases, supplies or possesses child pornography material or disseminates information about the performance of the above acts, through information systems, shall be punished by imprisonment of at least two years and a fine.' According to paragraph 6 of the same Article, imprisonment of up to three years is imposed to whoever knowingly acquires access to child pornography material through information technology systems. The 'notice-and-takedown' mechanism provided for in Article 14(5) as exposed above, is an ex post regulation of the issue. More measures must be taken towards the adoption of provisions particularly addressing the issue of spreading, sharing and

971 Article 2(2a), para.2 of the Greek law 2121/1993.
972 Wolfgang Benedek and Matthias C. Kettemann, Freedom of Expression and the Internet, page 92.
973 Article 21(1) of the Greek Constitution.
974 Wolfgang Benedek and Matthias C. Kettemann, Freedom of Expression and the Internet, page 93.

posting of personal information that pertain to children. Liability of Internet servers and intermediaries must be more severe if it is to protect childhood. It is not justified to maintain an overriding requirement of confidentiality if this prevents an effective investigation, for example in a case where an Internet service should have been obliged to disclose the identity of a person who had placed a sexual advertisement concerning a minor.[975]

10. How do you rank the access to freedom of expression online in your country?

Given the specific provision in Articles 34 and 35 the Greek Law No. 4624/2019 implementing measures of the European Regulation (EU) 2016/679, about the 'right to delete' and the 'right to object', the freedom of others' expression online gets automatically restricted in principle and in a timely horizon due to a legitimate reason of protection of personal data. However, the data subject's interest in the deletion should be considered significant in order for the content to be deleted finally, opening a window for a proportionality assessment and, thus, for respecting in the first the constitutionally enshrined Freedom of Expression. However, public interest exclusions also minify the personal data protection such as the exercise of official authority vested in the controller, reasons of public health, or defence of other legal claims resulting in rendering the Freedom of Expression online predominant if it genuinely serves the general benefit. This does not mean in any way that the subject's personal data lack in being respected. It rather signifies that whenever the person's privacy is accompanied by a role played in the public life, the general public is accredited with the right to have access to that information, and that the controller of the data cannot subsequently be held liable. In this regard, the Hellenic Authority for Data Protection has also developed its very own *res judicata* by expressly approving the fundamental right to Freedom of Expression, within its meaning as 'Freedom to receive and impart information and ideas' in Article 11 of the EU Charter of fundamental rights, which must be taken into account when evaluating requests of data subjects. From the aspect of the liability of internet intermediaries, the service providers are not generally forced by law to apply a general control to the online content and thus affecting the publishers' right to expression. Nevertheless, the judicial or administrative authority always keeps its jurisdiction to impose on the service provider the cessation or prevention of the alleged infringement. Besides, the service providers are being confronted with

[975] Internet: case law of the European Court of Human Rights, June 2015, page24 and 25.

an effort exercised by the Greek legislator to delimit their enjoyed immunity (see above in detail the special provisions of question 6). All in all, people are generally free to express their opinion through the Internet and they can post everything on it. The Internet content is taken down mostly in cases of infringement of intellectual property rights or in the case of infringement of personality. By explicit abomination, the freedom of expression online is sharply demarcated when criminal offences are at issue. The foregoing means that people in Greece can easily and freely express their opinion online as long as they are not violating other people's rights and they are not offending the public interest. Those rights are predicted specifically in the Constitutions for everyone to read. Sometimes, though, accusations of violations of other people's rights are being made on political grounds and not because there is a true violation of the right to Freedom of Expression. From 1 to 5 Greece is rated a '4'.

11. How do you overall assess the legal situation in your country regarding internet censorship?

In Greece, the Freedom of Expression though internet is not protected in a specific regulation rather in many different law texts. Although protected, this freedom has some limits. In Greece as censorship is defined the control exercised by an authority in the various manifestations of the thought and the art with the ultimate goal to prevent the exchange of information, ideas and opinions which are in contradiction with the principles of the authorities. The right to rreedom of expression on Internet conflicts with the right to protection of personal data or the intellectual property rights, but also the right to personality. In order to find out which right takes priority in every single case, the case law adopts the principle of the proportionality. So, at this part the Greek legislation is in accordance with the case law of the European Court of Human Rights and the case of the Court of the European Union.

There were some cases of censorship through internet with the most well-known that of Father Pastitsios and some other cases. It has shown that the Greek authorities are being pressed to take action against people who seem to make fun of situations that offend a certain group. Certainly, Greece is not the most tolerant country regarding the censorship, but she is also not in the worst ranking. It is certain that steps need to be made.

The most cases in Greece regarding the taking down or blocking of internet content referred to copyright violations and not violations of freedom of expression in general, but only in regard of someone other's personality. This

shows that fewer cases have been brought to justice concerning censorship issues and that fewer crimes have been committed.

The legal texts concerning the censorship are a bit inadequate. Of course, some progress has been made comparing with the previous years. Greece has amended its legislation incorporating the European Union Law, such as in the matter of the liability of

internet intermediaries. The right to freedom of expression is protected analogically from Article 14 of the Greek Constitution and there is not a specific regulation, controlling special issues arising from the use of technology in the expression of an opinion. So, we realise that the Greek legislation cannot deal with the peculiarity of the Internet, where the data are transferred very quickly. We could only claim that the Greek legislator by incorporating the regulations of the European Union has upgraded the protection of the beneficiaries of the Intellectual Property Rights As the use of technology rises and its uses change all the time, it would be logical and better for our government to make a specific regulation concerning the act and violation of rights through technology.

What can be said as a conclusion, regarding the protection against hate speech and the protection of freedom of expression against other rights, Greece has taken great steps in the recent years to align with the general European regulatory framework, not only in the criminal view of hate speech, but also in keeping with the new regulatory framework of the GDPR, safeguarding the protection of personal data and one's personality on the net. It is out of the question that the Greek Constitution in its Article 28 paragraph 1 recognises the predominance of the European and international law, thus abiding by the regulatory framework provided by the various laws and Conventions mentioned above for the protection against hate speech and the protection of other rights with regard to the exercise of the right to Freedom of Expression. Specific mentions to crimes committed via the net give rise to a new, more specific treatment established by the Law 4619/2019 towards the crimes conducted online. This detailed enumeration of specific instances of penalisation of human conduct on the net testimonies the will of the Greek legislation to further penalise the spread of hate speech taking place on the Internet. At the same time, the incorporation of the Regulation 2016/679/EU in the Greek law order is clear proof that the Greek legislation is fundamentally modernised in order to provide Internet users clear and specific treatment of their right to personality and their right to privacy and proportionate process of their personal data. As the world of the Internet evolves, further legislative measures must see the light of day, however the rudiments of the protection against hate speech are already set. The Greek law

order must always be vigilant for the changes to come in the close future and take the analogous measures as for the protection of other rights in the fast-pace development of the online environment.

Conclusion

In conclusion, the Greek national legislation regarding the control of the freedom of expression online is both following the membership trends by having already transposed the relevant European legislation and remaining identical at the same time by adopting national provisions. For example, the internet intermediaries enjoy, in principle, an immunity status. After the national legislator has transposed the Directive (EU) 2000/31 into the Greek legal order, the Article 14 of the Presidential Decree No. 131/2003 provides that not a general liability of the service providers to control the information exist. But, at the same time the internal legislation, first and before any other later, external efforts, invokes for a *per legem genus* (i.e. under certain genus of the law) responsibility of the service providers in view of delimiting their enjoyed immunity. However, except for the legislation for the intellectual property rights, there is no specific legislation in Greece as far as the Internet censorship concerned. Moreover, there is no specific legislation as far the self-regulation of the Internet content is concerned, but only some proposals. Nevertheless, we could say that there is a balance between the freedom of expression on the Internet and the protection of some fundamental rights of the users of the Internet. Overall, the legal context is deemed inadequate. There are no specific provisions targeting the takedown or block of internet content –just some scattered provisions concerning mainly violations of copyrights- whereas the Freedom of Expression is being regulated by an analogous application of the general provision of the constitution.

Table of legislation

Provision in Greek language	**Corresponding translation in English**
Άρθρο 14 του Ελληνικού συντάγματος	Article 14 of the Greek Constitution
1. Καθένας μπορεί να εκφράζει και να διαδίδει προφορικά, γραπτά και δια του τύπου τους στοχασμούς του τηρώντας τους νόμους του Κράτους.	1. Every person may express and propagate his thoughts orally, in writing and through the press in compliance with the laws of the State.
2. Ο τύπος είναι ελεύθερος. Η λογοκρισία και κάθε άλλο προληπτικό μέτρο απαγορεύονται.	2. The press is free. Censorship and all other preventive measures are prohibited.
3. Η κατάσχεση εφημερίδων και άλλων εντύπων, είτε πριν από την κυκλοφορία είτε ύστερα από αυτή, απαγορεύεται. Κατ' εξαίρεση επιτρέπεται η κατάσχεση, με παραγγελία του εισαγγελέα, μετά την κυκλοφορία: α) για προσβολή της χριστιανικής και κάθε άλλης γνωστής θρησκείας, β) για προσβολή του προσώπου του Προέδρου της Δημοκρατίας, γ) για δημοσίευμα που αποκαλύπτει πληροφορίες για τη σύνθεση, τον εξοπλισμό και τη διάταξη των ενόπλων δυνάμεων ή την οχύρωση της Χώρας ή που έχει σκοπό τη βίαιη ανατροπή του πολιτεύματος ή στρέφεται κατά της εδαφικής ακεραιότητας του Κράτους, δ) για άσεμνα δημοσιεύματα που προσβάλλουν ολοφάνερα τη δημόσια αιδώ, στις περιπτώσεις που ορίζει ο νόμος.	3. The seizure of newspapers and other publications before or after circulation is prohibited. Seizure by order of the public prosecutor shall be allowed exceptionally after circulation and in case of: a) an offence against the Christian or any other known religion, b) an insult against the person of the President of the Republic, c) a publication which discloses information on the composition, equipment and set-up of the armed forces or the fortifications of the country, or which aims at the violent overthrow of the regime or is directed against the territorial integrity of the State, d) an obscene publication which is obviously offensive to public decency, in the cases stipulated by law.
4. Σ' όλες τις περιπτώσεις της προηγούμενης παραγράφου ο εισαγγελέας, μέσα σε είκοσι τέσσερις ώρες από την κατάσχεση, οφείλει να υποβάλει την υπόθεση στο δικαστικό συμβούλιο, και αυτό, μέσα σε άλλες είκοσι τέσσερις ώρες, οφείλει να αποφασίσει για τη διατήρηση ή την άρση της κατάσχεσης, διαφορετικά η κατάσχεση αίρεται αυτοδικαίως. Τα ένδικα μέσα της έφεσης και της αναίρεσης επιτρέπονται στον εκδότη της εφημερίδας ή άλλου εντύπου που κατασχέθηκε και στον εισαγγελέα. **5. Καθένας ο οποίος θίγεται από ανακριβές δημοσίευμα ή εκπομπή έχει δικαίωμα απάντησης, το δε μέσο ενημέρωσης έχει αντιστοίχως υποχρέωση πλήρους και άμεσης	4. In all the cases specified under the preceding paragraph, the public prosecutor must, within twenty-four hours from the seizure, submit the case to the judicial council which, within the next twenty-four hours, must rule whether the seizure is to be maintained or lifted; otherwise it shall be lifted ipso jure. An appeal may be lodged with the Court of Appeals and the Supreme Civil and Criminal Court by the publisher of the newspaper or other printed matter seized and by the public prosecutor. ** 5. Every person offended by an inaccurate publication or broadcast has the right to reply, and the information medium has a corresponding obligation for full and

επανόρθωσης. Καθένας ο οποίος θίγεται από υβριστικό ή δυσφημιστικό δημοσίευμα ή εκπομπή έχει, επίσης, δικαίωμα απάντησης, το δε μέσο ενημέρωσης έχει αντιστοίχως υποχρέωση άμεσης δημοσίευσης ή μετάδοσης της απάντησης. Νόμος ορίζει τον τρόπο με τον οποίο ασκείται το δικαίωμα απάντησης και διασφαλίζεται η πλήρης και άμεση επανόρθωση ή η δημοσίευση και μετάδοση της απάντησης.	immediate redress. Every person offended by an insulting or defamatory publication or broadcast has also the right to reply, and the information medium has a corresponding obligation to immediately publish or transmit the reply. The manner in which the right to reply is exercised and in which full and immediate redress is assured or publication and transmission of the reply is made, shall be specified by law.
6. Το δικαστήριο, ύστερα από τρεις τουλάχιστον καταδίκες μέσα σε μία πενταετία για διάπραξη των εγκλημάτων που προβλέπονται στην παράγραφο 3, διατάσσει την οριστική ή προσωρινή παύση της έκδοσης του εντύπου και, σε βαριές περιπτώσεις, την απαγόρευση της άσκησης του δημοσιογραφικού επαγγέλματος από το πρόσωπο που καταδικάστηκε, όπως νόμος ορίζει Η παύση ή η απαγόρευση αρχίζουν αφότου η καταδικαστική απόφαση γίνει αμετάκλητη.	6. After at least three convictions within five years for the criminal acts defined under paragraph 3, the court shall order the definitive ban or the temporary suspension of the publication of the paper and, in severe cases, shall prohibit the convicted person from practising the profession of journalist as specified by law. The ban or suspension of publication shall be effective as of the date the court order becomes irrevocable.
**7. Νόμος ορίζει τα σχετικά με την αστική και ποινική ευθύνη του τύπου και των άλλων μέσων ενημέρωσης και με την ταχεία εκδίκαση των σχετικών υποθέσεων.	** 7. Matters relating to the civil and criminal liability of the press and of the other information media and to the expeditious trial of relevant cases, shall be specified by law.
8. Νόμος ορίζει τις προϋποθέσεις και τα προσόντα για την άσκηση του δημοσιογραφικού επαγγέλματος.	8. The conditions and qualifications requisite for the practice of the profession of journalist shall be specified by law.
**9. Το ιδιοκτησιακό καθεστώς, η οικονομική κατάσταση και τα μέσα χρηματοδότησης των μέσων ενημέρωσης πρέπει να γίνονται γνωστά, όπως νόμος ορίζει. Νόμος προβλέπει τα μέτρα και τους περιορισμούς που είναι αναγκαίοι για την πλήρη διασφάλιση της διαφάνειας και της πολυφωνίας στην ενημέρωση. Απαγορεύεται η συγκέντρωση του ελέγχου περισσότερων μέσων ενημέρωσης της αυτής ή άλλης μορφής. Απαγορεύεται ειδικότερα η συγκέντρωση περισσότερων του ενός ηλεκτρονικών μέσων ενημέρωσης της αυτής μορφής, όπως νόμος ορίζει. Η ιδιότητα του ιδιοκτήτη, του εταίρου, του βασικού μετόχου ή του διευθυντικού στελέχους επιχείρησης μέσων ενημέρωσης είναι	** 9. The ownership status, the financial situation and the means of financing of information media must be made known as specified by law. The measures and restrictions necessary for fully ensuring transparency and plurality in information shall be specified by law. The concentration of the control of more than one information media of the same type or of different types is prohibited. More specifically, concentration of more than one electronic information media of the same type is prohibited, as specified by law. The capacity of owner, partner, major shareholder or managing director of an information media enterprise, is incompatible with the capacity

ασυμβίβαστη με την ιδιότητα του ιδιοκτήτη, του εταίρου, του βασικού μετόχου ή του διευθυντικού στελέχους επιχείρησης που αναλαμβάνει έναντι του Δημοσίου ή νομικού προσώπου του ευρύτερου δημόσιου τομέα την εκτέλεση έργων ή προμηθειών ή την παροχή υπηρεσιών. Η απαγόρευση του προηγούμενου εδαφίου καταλαμβάνει και κάθε είδους παρένθετα πρόσωπα, όπως συζύγους, συγγενείς, οικονομικά εξαρτημένα άτομα ή εταιρείες. Νόμος ορίζει τις ειδικότερες ρυθμίσεις, τις κυρώσεις που μπορεί να φθάνουν μέχρι την ανάκληση της άδειας ραδιοφωνικού ή τηλεοπτικού σταθμού και μέχρι την απαγόρευση σύναψης ή την ακύρωση της σχετικής σύμβασης, καθώς και τους τρόπους ελέγχου και τις εγγυήσεις αποτροπής των καταστρατηγήσεων των προηγούμενων εδαφίων.	of owner, partner, major shareholder or managing director of an enterprise that undertakes towards the Public Administration or towards a legal entity of the wider public sector to perform works or to supply goods or services. The prohibition of the previous section extends also over all types of intermediary persons, such as spouses, relatives, financially dependent persons or companies. The specific regulations, the sanctions, which may extend to the point of revocation of the license of a radio or television station and to the point of prohibition of the conclusion or to the annulment of the pertinent contract, as well as the means of control and the guarantees for the prevention of infringements of the previous sections, shall be determined by law.
Άρθρο 15 του Ελληνικού Συντάγματος	Article 15 of the Greek Constitution
1. Οι προστατευτικές για τον τύπο διατάξεις του προηγούμενου άρθρου δεν εφαρμόζονται στον κινηματογράφο, τη φωνογραφία, τη ραδιοφωνία, την τηλεόραση και κάθε άλλο παρεμφερές μέσο μετάδοσης λόγου ή παράστασης.	1. The protective provisions for the press in the preceding Article shall not be applicable to films, sound recordings, radio, television or any other similar medium for the transmission of speech or images.
**2. Η ραδιοφωνία και η τηλεόραση υπάγονται στον άμεσο έλεγχο του Κράτους. Ο έλεγχος και η επιβολή των διοικητικών κυρώσεων υπάγονται στην αποκλειστική αρμοδιότητα του Εθνικού Συμβουλίου Ραδιοτηλεόρασης που είναι ανεξάρτητη αρχή, όπως νόμος ορίζει. Ο άμεσος έλεγχος του Κράτους, που λαμβάνει και τη μορφή του καθεστώτος της προηγούμενης άδειας, έχει ως σκοπό την αντικειμενική και με ίσους όρους μετάδοση πληροφοριών και ειδήσεων, καθώς και προϊόντων του λόγου και της τέχνης, την εξασφάλιση της ποιοτικής στάθμης των προγραμμάτων που επιβάλλει η κοινωνική αποστολή της ραδιοφωνίας και της τηλεόρασης και η πολιτιστική ανάπτυξη της Χώρας, καθώς και το σεβασμό της αξίας του ανθρώπου και την προστασία της παιδικής ηλικίας και της νεότητας. Νόμος ορίζει τα σχετικά με την υποχρεωτική και δωρεάν μετάδοση των εργασιών της	** 2. Radio and television shall be under the direct control of the State. The control and imposition of administrative sanctions belong to the exclusive competence of the National Radio and Television Council, which is an independent authority, as specified by law. The direct control of the State, which may also assume the form of a prior permission status, shall aim at the objective and on equal terms transmission of information and news reports, as well as of works of literature and art, at ensuring the quality level of programs mandated by the social mission of radio and television and by the cultural development of the Country, as well as at the respect of the value of the human being and the protection of childhood and youth. Matters relating to the mandatory and free of charge transmission of the workings of the Parliament and of its committees, as well as of the electoral campaign messages of the

Βουλής και των επιτροπών της, καθώς και προεκλογικών μηνυμάτων των κομμάτων από τα ραδιοτηλεοπτικά μέσα.	political parties by radio and television, shall be specified by law.
Άρθρο 5Ατου Ελληνικού Συντάγματος 1. Καθένας έχει δικαίωμα στην πληροφόρηση, όπως νόμος ορίζει. Περιορισμοί στο δικαίωμα αυτό είναι δυνατόν να επιβληθούν με νόμο μόνο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων. 2. Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19.	** Article 5A of the Greek Constitution 1. All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties. 2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of Articles 9, 9A and 19
Άρθρο 367 παράγραφος 1 του Ελληνικού Ποινικού Κώδικα 1. Δεν αποτελούν άδικη πράξη: α) οι δυσμενείς κρίσεις για επιστημονικές, καλλιτεχνικές ή επαγγελματικές εργασίες· β) οι δυσμενείς εκφράσεις που περιέχονται σε έγγραφο δημόσιας αρχής για αντικείμενα που ανάγονται στον κύκλο της υπηρεσίας της, καθώς και γ) οι εκδηλώσεις που γίνονται για την εκτέλεση νόμιμων καθηκόντων, την άσκηση νόμιμης εξουσίας ή για τη διαφύλαξη (προστασία) δικαιώματος ή από άλλο δικαιολογημένο ενδιαφέρον ή δ) σε ανάλογες περιπτώσεις.	Article 367 paragraph 1 of the Greek penal Code the adverse judgments and manifestations do not constitute illegal acts when they are being made due to a legal performance of duty, the exercise of legitimate force protection of rights or another justified interest
Άρθρο 18 νόμου 4267/2014 παράγραφος 1 1.Με διάταξη του αρμόδιου εισαγγελέα πρωτοδικών ή του εισαγγελέα εφετών, εάν η υπόθεση εκκρεμεί στο εφετείο, διατάσσεται η κατάργηση ιστοσελίδας, η οποία φιλοξενείται στην Ελλάδα και περιέχει ή διαδίδει υλικό παιδικής πορνογραφίας. Η διάταξη αυτή πρέπει να είναι ειδικώς και πλήρως αιτιολογημένη, κοινοποιείται στον πάροχο υπηρεσιών φιλοξενίας της εν λόγω ιστοσελίδας και εκτελείται αμέσως	Article 18 in Law 4267/2014 paragraph 1 the Public Prosecutor has the right the elimination of a hosted website in Greece that ether contains either transmits child pornography material

Άρθρο 7 Νόμου 3603/2007 παράγραφος 1 Διενέργεια και δημοσιοποίηση δημοσκοπήσεων κατά την προεκλογική περίοδο1.α)Δεκαπέντε (15) ημέρες πριν από τη διενέργεια των βουλευτικών εκλογών, των εκλογών για την ανάδειξη αντιπροσώπων στο Ευρωπαϊκό Κοινοβούλιο και των δημοψηφισμάτων και έως την 19.00 ώρα της ημέρας της ψηφοφορίας, απαγορεύεται η δημοσιοποίηση δημοσκοπήσεων για την πρόθεση ψήφου των εκλογέων και η καθ' οιονδήποτε τρόπο μετάδοση αποτελεσμάτων των δημοσκοπήσεων, καθώς και η καθ' οιονδήποτε τρόπο μετάδοση και αναμετάδοσή τους από τα μέσα ενημέρωσης, με οποιονδήποτε τρόπο και αν διανέμονται ή εκπέμπουν.	Article 7 paragraphs 1 of the Law 3603/2007 15 days before the parliamentary, European elections and the referendum it is forbidden to publicise the polls and until the 7 o clock the day of the election it is forbidden to publicise the polls about the vote intentions of the electors. Furthermore it prohibits: the publication of the result of the elections as well as with any means the transmission and retransmission from the media.
Προεδρικό διάταγμα 131/2003 άρθρο 13 Σε περίπτωση παροχής μιας υπηρεσίας της κοινωνίας της πληροφορίας συνισταμένης στην αποθήκευση πληροφοριών παρεχομένων από ένα αποδέκτη υπηρεσίας, δεν υφίσταται ευθύνη του φορέα παροχής της υπηρεσίας για τις πληροφορίες που αποθηκεύονται μετά από αίτηση αποδέκτη της υπηρεσίας, υπό τους όρους ότι: (α) ο φορέας παροχής της υπηρεσίας δεν γνωρίζει πραγματικά ότι πρόκειται για παράνομη δραστηριότητα ή πληροφορία και ότι, σε ό,τι αφορά αξιώσεις αποζημιώσεως , δεν γνωρίζει τα γεγονότα ή τις περιστάσεις από τις οποίες προκύπτει η παράνομη δραστηριότητα ή πληροφορία, ή (β) ο φορέας παροχής της υπηρεσίας, μόλις αντιληφθεί τα προαναφερθέντα , αποσύρει ταχέως τις πληροφορίες ή καθιστά την πρόσβαση σε αυτές αδύνατη. 2. Η παράγραφος 1 δεν εφαρμόζεται όταν ο αποδέκτης της υπηρεσίας ενεργεί υπό την εξουσία ή υπό τον έλεγχο του φορέα παροχής της υπηρεσίας. 3. Το παρόν άρθρο δεν θίγει τη δυνατότητα να επιβληθεί δικαστικά ή διοικητικά στο φορέα παροχής υπηρεσιών η παύση ή η πρόληψη της παράβασης.	Presidential Decree 131/2003 Article 13 In the event of an information society service consisting of storing information provided by a recipient of the service, the service provider shall not be responsible for the information stored at the request of the recipient of the service, under the conditions that: (a) the service provider does not really know that it is an illegal activity or information and that, as far as compensation claims are concerned, he is not aware of the facts or circumstances resulting from the illegal activity or information, or (b) the service provider, as soon as it is aware of the above, rapidly withdraws the information or makes it impossible to access. 2. Paragraph 1 shall not apply where the recipient of the service is acting under the authority or control of the service provider. 3. This Article shall be without prejudice to the possibility for the service provider to bring an action to cease or prevent the infringement
Προεδρικό διάταγμα 131/2003 άρθρο 14 1. Οι φορείς παροχής υπηρεσιών δεν έχουν, για την παροχή υπηρεσιών που αναφέρονται στα άρθρα 11, 12 και 13 του παρόντος γενική	Presidential Decree 131/2003 Article 14 1. Service providers shall not have the general obligation to control the information transmitted or stored for the

υποχρέωση ελέγχου των πληροφοριών που μεταδίδουν ή αποθηκεύουν ούτε γενική υποχρέωση δραστήριας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν ότι πρόκειται για παράνομες δραστηριότητες. 2. Χωρίς να παραβιάζονται οι διατάξεις περί προστασίας του απορρήτου και των προσωπικών δεδομένων, οι φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας είναι υποχρεωμένοι να ενημερώνουν πάραυτα τις αρμόδιες κρατικές αρχές για τυχόν υπόνοιες περί χορηγουμένων παράνομων πληροφοριών ή δραστηριοτήτων που επιχειρούν αποδέκτες των υπηρεσιών τους, και να ανακοινώνουν στις αρμόδιες αρχές κατ' αίτησή τους πληροφορίες που διευκολύνουν την εντόπιση αποδεκτών των υπηρεσιών τους με τους οποίους έχουν συμφωνίες αποθήκευσης.	services referred to in Articles 11, 12 and 13 of this General Act or the general obligation to actively seek out facts or circumstances which show that these are illegal activities. 2. Without prejudice to the provisions on the protection of confidentiality and personal data, information society service providers shall be obliged to immediately inform the competent state authorities of any suspicions of unlawful information or activities being attempted by recipients of their services, and communicate to the competent authorities at their request information which facilitates the identification of recipients of their services with whom they have storage agreements.
Νόμος 4072/2012 άρθρο 153, παράγραφοι 1 και 2 1. Όποιος έχει αξίωση για άρση και παράλειψη λόγω προσβολής του σήματος μπορεί να ζητήσει και τη λήψη ασφαλιστικών μέτρων. 2. Ο δικαιούχος του σήματος μπορεί να ζητήσει τη συντηρητική κατάσχεση ή την προσωρινή απόδοση των εμπορευμάτων με το προσβάλλον διακριτικό γνώρισμα προκειμένου να εμποδιστεί η είσοδος ή η κυκλοφορία τους στο δίκτυο εμπορικής διανομής.	Law No 4072/2012, Article 153, paragraphs 1 and 2 1. Anyone claiming for removal or failure to infringe the mark may also seek interim measures. 2. The proprietor of a trade mark may request the seizure or temporary restitution of the infringing goods in order to prevent their entry or circulation in the commercial distribution network.
Νόμος 4072/2012 άρθρο 154, παράγραφος 1 Εφόσον επαρκώς πιθανολογείται με ευλόγως διαθέσιμα αποδεικτικά στοιχεία προσβολή ή επικείμενη προσβολή του σήματος και κάθε καθυστέρηση μπορεί να προκαλέσει ανεπανόρθωτη ζημία στον δικαιούχο του σήματος ή υπάρχει αποδεδειγμένος κίνδυνος καταστροφής των αποδεικτικών στοιχείων, το μονομελές πρωτοδικείο μπορεί να διατάσσει ως ασφαλιστικό μέτρο τη συντηρητική κατάσχεση των παράνομων προϊόντων που κατέχονται από τον καθού και, εφόσον ενδείκνυται, των υλικών και των εργαλείων που αποτελούν μέσο τέλεσης ή προϊόν ή απόδειξη της προσβολής. Αντί για συντηρητική	Law 4072/2012 Rule 154 (1) Where sufficiently probable evidence of an infringement or impending infringement of the mark is reasonably available and any delay may cause irreparable damage to the proprietor of the mark or there is a proven risk of destruction of the evidence, the unilateral court may order, as a precautionary measure, the preventive confiscation of the unlawful products held by the defendant and, where appropriate, the materials and tools which constitute the means of enforcement; or products or evidence of infestation. Instead of conservative seizure, the court may order

κατάσχεση το δικαστήριο μπορεί να διατάξει την αναλυτική απογραφή των αντικειμένων αυτών, καθώς και τη φωτογράφισή τους, τη λήψη δειγμάτων των ανωτέρω προϊόντων, καθώς και σχετικών εγγράφων. Στις παραπάνω περιπτώσεις το δικαστήριο μπορεί να συζητήσει την αίτηση χωρίς να κλητεύσει εκείνον κατά του οποίου απευθύνεται προσωρινή διαταγή κατά το άρθρο 691 παράγραφος 2 του Κώδικα Πολιτικής Δικονομίας.	the detailed inventory of these objects, as well as their photographing, the taking of samples of the above products, and related documents. In the above cases the court may hear the application without summoning the person against whom a provisional order is made under Article 691 (2) of the Code of Civil Procedure.
Άρθρο 682 Πολιτική Δικονομία Κατά την ειδική διαδικασία των άρθρων 683 έως 703 τα δικαστήρια, σε επείγουσες περιπτώσεις ή για να αποτραπεί επικείμενος κίνδυνος, μπορούν να διατάζουν ασφαλιστικά μέτρα για την εξασφάλιση ή διατήρηση ενός δικαιώματος ή τη ρύθμιση μιας κατάστασης και να τα μεταρρυθμίζουν ή να τα ανακαλούν. Το δικαίωμα είναι δυνατό να εξαρτάται από αίρεση ή προθεσμία ή να αφορά μέλλουσα απαίτηση. 2. Τα ασφαλιστικά μέτρα μπορούν να διαταχθούν και κατά τη διάρκεια της δίκης που αφορά την κύρια υπόθεση.	Article 682 Civil Procedure Under the special procedure provided for in Articles 683 to 703, in emergency cases or in order to prevent imminent danger, courts may order interim measures to safeguard or preserve a right or to regulate a situation and to reform or enforce them. The right may be subject to a term or term or to a future claim. 2. The application for interim measures may also be ordered during the proceedings in the main proceedings.
Άρθρο 25, παράγραφος 3 του ελληνικού Συντάγματος Η καταχρηστική άσκηση δικαιώματος δεν επιτρέπεται.	Article 25, paragraph 3 of the Greek Constitution The abusive exercise of rights is not permitted.
Άρθρο 20, παράγραφος 1 του νόμου 4624/2019 1. Οι κανονιστικές αποφάσεις και οι ατομικές διοικητικές πράξεις της Αρχής, συμπεριλαμβανομένων των αποφάσεων με τις οποίες επιβάλλονται κυρώσεις, προσβάλλονται με αίτηση ακυρώσεως ενώπιον του Συμβουλίου της Επικρατείας.	Article 20, paragraph 1 of the Greek Law No. 4624/2019 The regulatory decisions and the individual administrative acts, included of the decisions by which sanctions are imposed, can be brought before the Council of State with an application for annulment.
Άρθρο 28, παράγραφος 1 του νόμου 4624/2019 1. Στον βαθμό που είναι αναγκαίο να συμβιβαστεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και	Article 28, paragraph 1 of the Greek Law No. 4624/2019 If it is necessary for the compliance of the freedom to protection of personal data with the right to Freedom of Expression and information, including processing for

πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς και για σκοπούς ακαδημαϊκής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται όταν: α) το υποκείμενο των δεδομένων έχει παράσχει τη ρητή συγκατάθεσή του, β) αφορά δεδομένα προσωπικού χαρακτήρα που έχουν προδήλως δημοσιοποιηθεί από το ίδιο το υποκείμενο, γ) υπερέχει το δικαίωμα στην ελευθερία της έκφρασης και το δικαίωμα της πληροφόρησης έναντι του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα του υποκειμένου, ιδίως για θέματα γενικότερου ενδιαφέροντος ή όταν αφορά δεδομένα προσωπικού χαρακτήρα δημοσίων προσώπων και δ) όταν περιορίζεται στο αναγκαίο μέτρο για την εξασφάλιση της ελευθερίας της έκφρασης και του δικαιώματος ενημέρωσης, ιδίως όταν αφορά ειδικών κατηγοριών δεδομένα Προσωπικού Χαρακτήρα, καθώς και ποινικές διώξεις, καταδίκες και τα σχετικά με αυτές μέτρα ασφαλείας, λαμβάνοντας υπόψη το δικαίωμα του υποκειμένου στην ιδιωτική και οικογενειακή του ζωή.	journalistic purposes and the purposes of academic, artistic or literary expression, the processing of the personal data is permitted, when: a)the subject of the personal data has given his expressed consent, b)the subject of the personal data has made them public, c) the right to protect the Freedom of Expression and information prevail of the right to protect the personal data, especially when it is about a general issue or it is about the personal data of a public person, d) it is limited to the necessary measure in order to the Freedom of Expression and information be satisfied, too, especially when it is about special categories of personal data and criminal proceedings, convictions and security measures, taking into account the right of the subject to personal and family life.
Άρθρο 66Ε του Νόμου 2121/1993 1. Αν προσβάλλεται στο διαδίκτυο δικαίωμα πνευματικής ιδιοκτησίας ή συγγενικό δικαίωμα, ο δικαιούχος μπορεί να ακολουθήσει την περιγραφόμενη στις επόμενες παραγράφους διαδικασία. Ως δικαιούχος για τις ανάγκες του παρόντος άρθρου νοείται ο δικαιούχος του οποίου το δικαίωμα προσβάλλεται στο διαδίκτυο, καθώς και οποιοσδήποτε οργανισμός συλλογικής διαχείρισης ή προστασίας, στον οποίο έχει ανατεθεί η διαχείριση ή η προστασία δικαιωμάτων πνευματικής ιδιοκτησίας ή συγγενικών δικαιωμάτων. Η παρούσα διαδικασία δεν εφαρμόζεται στις περιπτώσεις προσβολών που τελούνται από τελικούς χρήστες με την τηλεφόρτωση έργων (downloading) ή με τη ρευμάτωση δεδομένων συνεχούς ροής (streaming) ή σε περιπτώσεις ανταλλαγής αρχείων μέσω ομότιμων δικτύων (peertopeer), οι οποίες επιτρέπουν την απευθείας ανταλλαγή μεταξύ τελικών χρηστών έργων σε ψηφιακή μορφή ή σε περιπτώσεις παροχής υπηρεσιών	Article 66E of the Greek Law No. 2121/1993 1. In cases of copyright or related rights infringement on the internet, the right holder may follow the procedure provided for in the paragraphs herein. For the purposes of this Article, by right holder is meant the right holder whose right is infringed on the internet as well as any collective management organisation or collective protection organisation to which has been assigned the collective management or protection of copyright or related rights. Such procedure shall not apply neither to cases of infringement committed by end users by means of downloading of works or streaming or peer to peer exchange of files, which allow for the direct exchange of digital files of works between end users, nor to cases of infringement by means of provision of data storing services through cloud computing. This procedure shall be without prejudice to the procedure provided for in the Regulation on Management and Assignment

αποθήκευσης δεδομένων με την τεχνική υπολογιστικού νέφους (cloudcomputing). Η παρούσα διαδικασία δεν θίγει τη διαδικασία που προβλέπεται από τον Κανονισμό Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (domainnames) με κατάληξη .gr της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), ο οποίος καταρτίζεται με απόφαση της ΕΕΤΤ.	of .gr Domain names of the Hellenic Telecommunications and Post Commission (EETT), which is specified by EETT's decision.
2. Για την εφαρμογή της διαδικασίας που προβλέπεται στο παρόν άρθρο συνιστάται, με απόφαση του Υπουργού Πολιτισμού και Αθλητισμού, Επιτροπή για τη γνωστοποίηση διαδικτυακής προσβολής δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων, η οποία συνεπικουρείται από το προσωπικό του ΟΠΙ. Η Επιτροπή είναι τριμελής και αποτελείται από τον πρόεδρο του Διοικητικού Συμβουλίου του ΟΠΙ με αναπληρωτή του τον αντιπρόεδρο του Διοικητικού Συμβουλίου του ΟΠΙ, έναν εκπρόσωπο της ΕΕΤΤ και τον αναπληρωτή του, που τους ορίζει ο πρόεδρος της ΕΕΤΤ, έναν εκπρόσωπο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και τον αναπληρωτή του, οριζόμενους από τον Πρόεδρο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Πρόεδρος της Επιτροπής είναι ο πρόεδρος του ΟΠΙ και γραμματέας είναι ο εκπρόσωπος της ΕΕΤΤ. Η Επιτροπή έχει τριετή θητεία.	2. In order for the procedure provided for in this Article to have effect, a Committee is formed by decision of the Minister of Culture and Sports for the notification of copyright and related rights infringement on the internet. This Committee shall be assisted by the Hellenic Copyright Organisation (HCO) staff. It shall be a three member Committee consisting of HCO's Administrative Board President substituted with HCO's Administrative Board Vice President, an EETT delegate and his substitute as designated by EETT's President, and a delegate of the Hellenic Data Protection Authority (HDPA) and his substitute as designated by HDPA's President. President of the Committee shall be HCO's President and the EETT's delegate shall be its secretary. The Committee shall have a three (3) year term.
3. Με απόφαση του Υπουργού Πολιτισμού και Αθλητισμού καθορίζεται κάθε θέμα σχετικό με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες της Επιτροπής. Για τον καθορισμό της αμοιβής των συμμετεχόντων στην Επιτροπή ισχύουν οι διατάξεις του άρθρου 21 του ν. 4354/2015 (Α' 176), όπως τροποποιήθηκαν με τις όμοιες του άρθρου 52 του ν. 4369/2016 (Α' 33). Στην απόφαση του πρώτου εδαφίου καθορίζεται και το τέλος που καταβάλλει ο ενδιαφερόμενος υπέρ του ΟΠΙ μαζί με την αίτησή του στην Επιτροπή ως τέλος εξέτασης της υπόθεσής του. Το τέλος αυτό προκαταβάλλεται και αποτελεί απαραίτητη προϋπόθεση έναρξης της διαδικασίας.	3. By decision of the Minister of Culture and Sports shall be determined the forming, functions and competence of the Committee and any relevant matter. The provisions of Article 21 of law 4354/2015 (A'176) as amended by those of Article 52 of law 4369/2016 (A'33) shall apply to determine the compensation fee payable to the members of the Committee. The decision of sentence 1 herein shall also determine, as a review fee, the fee payable to HCO by the applicant in conjunction with his application to the Committee. Such fee shall be paid in advance and shall be a prerequisite for the commencement of the procedure.
4. Ο δικαιούχος υποβάλλει στην Επιτροπή αίτηση είτε αυτοπροσώπως είτε ηλεκτρονικά	4. The right holder shall submit his application for termination of infringement

για άρση της προσβολής. Συμπληρώνει την ειδικά προδιατυπωμένη και αναρτημένη στην ιστοσελίδα του ΟΠΙ αίτηση προς την Επιτροπή, στην οποία επισυνάπτει κάθε έγγραφο που αναφέρεται σε αυτήν ως υποχρεωτικό, καθώς και κάθε άλλο στοιχείο πρόσφορο να αποδείξει το δικαίωμά του. Προϋπόθεση του παραδεκτού υποβολής της αίτησης είναι ο δικαιούχος να έχει κάνει χρήση της αντίστοιχης διαδικασίας που προβλέπεται από τον πάροχο και η διαδικασία αυτή, ενώ έχει ολοκληρωθεί εντός εύλογου χρόνου, να μην έχει τελεσφορήσει.	either in person or electronically. He shall fill in the pro-forma application to the Committee, which is available on HCO's website. Attached to this he shall submit all and any document referred to therein as mandatory as well as any additional evidence that may establish his right. For the submission of the application to be admissible, the right holder must have made use of the corresponding procedure which the provider had determined and which was concluded within reasonable time but with no result.
5. Η Επιτροπή εντός δέκα (10) εργάσιμων ημερών από τη λήψη της αίτησης αποφασίζει είτε: α) να θέσει την υπόθεση στο αρχείο είτε β) να συνεχίσει τη διαδικασία. α) Η υπόθεση τίθεται στο αρχείο με πράξη της Επιτροπής, στην οποία αναφέρονται τουλάχιστον ένας από τους ακόλουθους λόγους: αα) μη χρήση της προδιατυπωμένης αίτησης, ββ) έλλειψη επαρκούς πληροφόρησης, γγ) ύπαρξη εκκρεμοδικίας μεταξύ των ίδιων μερών ή έκδοση οριστικής απόφασης επί της εξεταζόμενης διαφοράς, δδ) έλλειψη αρμοδιότητας, εε) έλλειψη λόγων και επαρκών αποδεικτικών στοιχείων (προδήλως αβάσιμη), στστ) απόσυρση της αίτησης πριν από την εξέτασή της, ζζ) μη καταβολή του τέλους εξέτασης της υπόθεσης σύμφωνα με την παράγραφο 3 και, ηη) λήψη άδειας χρήσης δικαιωμάτων. β) Αν συνεχιστεί η διαδικασία, η Επιτροπή ενημερώνει ταυτόχρονα εντός δέκα (10) εργάσιμων ημερών από τη λήψη της αίτησης τους παρόχους πρόσβασης στο διαδίκτυο και, όπου είναι εφικτό, τον πάροχο υπηρεσίας φιλοξενίας και τους διαχειριστές ή/και τους ιδιοκτήτες των αναφερόμενων στην αίτηση ιστοσελίδων. Η γνωστοποίηση αυτή περιλαμβάνει τουλάχιστον τον ακριβή προσδιορισμό των δικαιωμάτων που υποστηρίζεται ότι προσβάλλονται, τις διατάξεις του νόμου που κατά δήλωση του δικαιούχου παραβιάζονται, περίληψη των γεγονότων και των αποτελεσμάτων της αξιολόγησης των αποδεικτικών στοιχείων, το αρμόδιο πρόσωπο προς το οποίο μπορεί να υποβληθούν αντιρρήσεις, τους όρους τερματισμού της διαδικασίας και αναφορά της δυνατότητας εκούσιας συμμόρφωσης των εμπλεκομένων. Ο αποδέκτης της ως άνω	5. Within ten (10) working days from receipt of the application, the Committee shall either (a) archive the case or (b) follow through the procedure. a. The case shall be archived by means of a Committee act in which mention shall be made of one of the following reasons: aa. Non-use of pro-forma application bb. Lack of sufficient information cc. a case is pending between the same parties before the courts or the issuance of a final decision on the dispute at issue dd. lack of competence ee. Lack of grounds and lack of sufficient evidence (-apparently unsubstantiated-) ff. withdrawal from the application prior to its review gg. Non-payment of the review fee pursuant to the provisions of paragraph 3 above. hh. Obtaining a license of use b. If the procedure follows through, within ten (10) working days from receipt of the application, the Committee shall simultaneously notify the internet access providers and, where possible, the host providers and administrators, and/or proprietors of the websites referred to in the application. Such notice thereof shall include at least the exact definition of the rights allegedly infringed; the law provisions which, by declaration of the rightholder, are violated; a summary of events and the outcome of the evaluation of evidence; the competent person to whom objections may be raised; the conditions upon which the procedure may be terminated and a mention to the voluntary compliance for which the parties involved may opt. The person which receives such notice may voluntary comply to the applicant's claim or obtain from the

γνωστοποίησης μπορεί να συμμορφωθεί εκουσίως στο αίτημα του αιτούντος ή να λάβει από αυτόν τη σχετική άδεια εντός δέκα (10) εργάσιμων ημερών από την ημερομηνία της λήψης της γνωστοποίησης. Εναλλακτικά μπορεί να υποβάλει αντιρρήσεις στην Επιτροπή εντός πέντε (5) εργάσιμων ημερών από την ημερομηνία της λήψης της γνωστοποίησης αποστέλλοντας ταυτόχρονα όλα τα αποδεικτικά στοιχεία, από τα οποία προκύπτει, ιδίως, ότι δεν υφίσταται προσβολή. Οι προθεσμίες αυτές μπορούν να παραταθούν ως το διπλάσιο με απόφαση της Επιτροπής. Στην περίπτωση της εκούσιας συμμόρφωσης του αποδέκτη της γνωστοποίησης εκδίδεται απόφαση της Επιτροπής στην οποία αναφέρεται ρητά η οικειοθελής συμμόρφωσή του. Στην περίπτωση της λήψης άδειας χρήσης δικαιωμάτων η υπόθεση τίθεται στο αρχείο. Μετά τη λήξη της προθεσμίας για υποβολή αντιρρήσεων και όπου κρίνεται απαραίτητο, η Επιτροπή αιτείται από οποιοδήποτε μέρος την προσκόμιση επιπλέον στοιχείων εντός πέντε (5) εργάσιμων ημερών.	applicant a relevant permission within ten (10) working days from the date of receipt of the notice. In any other case, he may raise his objections to the Committee within five (5) working days from the date of receipt of the notice whereby he shall simultaneously produce all evidence that explicitly proves that no infringement thereby occurs. Such deadlines may extend to the double upon decision by the Committee. In the case that the person who receives the notice voluntary complies with it, a decision by the Committee is issued in which his voluntary compliance is expressly stated. In the event that a license for use of rights is obtained the case shall be archived. Upon expiration of the deadline for objections to be raised and where deemed necessary the Committee shall ask further evidence to be submitted within five (5) working days.
6. Η Επιτροπή εντός πέντε (5) εργάσιμων ημερών από τη λήξη των ανωτέρω προθεσμιών εξετάζει την υπόθεση και το αργότερο εντός σαράντα (40) εργάσιμων ημερών από την υποβολή της αίτησης κοινοποιεί στους αποδέκτες τής γνωστοποίησης και στον αιτούντα απόφαση με την οποία: α) είτε θέτει την υπόθεση στο αρχείο με αιτιολογημένη πράξη της, αν δεν διαπιστωθεί προσβολή δικαιώματος πνευματικής ιδιοκτησίας ή/και συγγενικών δικαιωμάτων, β) είτε, αν διαπιστωθεί προσβολή, εκδίδει αιτιολογημένη απόφασή της, με την οποία καλεί τους αποδέκτες αυτής να συμμορφωθούν με αυτήν εντός προθεσμίας όχι μεγαλύτερης των τριών (3) εργάσιμων ημερών από την επίδοσή της προς αυτούς. Σε περίπτωση που οι προθεσμίες της παραγράφου 5 παραταθούν με απόφαση της Επιτροπής βάσει του έβδομου εδαφίου της, η προθεσμία των σαράντα (40) εργασίμων ημερών του πρώτου εδαφίου της παρούσας επεκτείνεται σε εξήντα (60) εργάσιμες ημέρες. Εάν η Επιτροπή διαπιστώσει ότι το δικαίωμα πνευματικής ιδιοκτησίας ή το συγγενικό δικαίωμα προσβάλλεται, καλεί τους αποδέκτες της γνωστοποίησης να	6. Within five (5) working days from expiration of the above deadlines the Committee shall review the case and in no later than forty (40) working days from the submission of the application, it shall notify of its decision the applicant and the person who receives the notice. In such decision: a. Where no infringement of copyright or related rights is substantiated, it shall archive the case by issuing a reasoned opinion. b. Where an infringement is substantiated, it shall issue a reasoned decision in which it shall ask from all those that receive it to comply with it within a period of no more than three (3) working days from the date of receipt by them. In case that the deadlines set out in paragraph 5 above are extended by decision of the Committee pursuant to the provisions of sentence 7 thereof, the deadline of forty (40) working days referred to in sentence 1 herein shall be extended to sixty (60) working days. Where the Committee substantiates that copyright or related rights are infringed, it shall ask from those that are notified to remove the infringing content from the website where it has been illegally posted or to block access

απομακρύνουν το περιεχόμενο που προσβάλλει το δικαίωμα από την ιστοσελίδα στην οποία αυτό έχει αναρτηθεί παράνομα ή να διακόψουν την πρόσβαση σε αυτό. Εάν η ιστοσελίδα στην οποία βρίσκεται το περιεχόμενο φιλοξενείται σε διακομιστή (server) που βρίσκεται εντός της ελληνικής επικράτειας, η Επιτροπή καλεί τους αποδέκτες της γνωστοποίησης να απομακρύνουν το συγκεκριμένο περιεχόμενο. Σε περίπτωση προσβολών μεγάλης κλίμακας, η Επιτροπή μπορεί να αποφασίσει αντί για την απομάκρυνση του περιεχομένου διακοπή της πρόσβασης σε αυτό. Αν η ιστοσελίδα φιλοξενείται σε διακομιστή εκτός της ελληνικής επικράτειας, η Επιτροπή καλεί τον πάροχο πρόσβασης στο διαδίκτυο να διακόψει την πρόσβαση στο περιεχόμενο.	to it. Where the content is hosted on a website whose server is within the Greek territory, the Committee shall ask from those that are notified the removal of such content. In case of large scale infringement the Committee may decide, instead of content removal, the blocking of access to this content. Where the website is hosted on a server outside the Greek territory, the Committee shall ask the internet access provider to block access to this content.
7. Σε περίπτωση μη συμμόρφωσης προς το διατακτικό της απόφασης, η Επιτροπή επιβάλλει πρόστιμο ποσού πεντακοσίων (500) έως χιλίων (1.000) ευρώ για κάθε ημέρα μη συμμόρφωσης. Μεταξύ των κριτηρίων που λαμβάνονται υπόψη είναι η βαρύτητα της προσβολής και η επανάληψή της. Με κοινή απόφαση των Υπουργών Οικονομικών και Πολιτισμού και Αθλητισμού καθορίζονται η διαδικασία επιβολής και είσπραξης του προστίμου, οι αρμόδιες υπηρεσίες είσπραξης, καθώς και κάθε άλλο σχετικό θέμα.	7. In case of non-compliance with the dictum of the decision, the Committee shall impose a fine of five hundred (500) up to a thousand (1000) Euros for each and every day of noncompliance. The seriousness of the infringement and its repetition shall be amongst the criteria taken into account. The Minister of Finances in conjunction with the Minister of Culture and Sports shall mutually decide on the manner in which the fine shall be imposed and collected, the competent collection authorities and all other relevant matters.
8. Η έναρξη της διαδικασίας ενώπιον της Επιτροπής δεν αναστέλλει ούτε επηρεάζει την άσκηση αξιώσεων για την ίδια διαφορά ενώπιον των δικαστηρίων. Αν όμως έχει ασκηθεί προσφυγή από τον ίδιο αιτούντα με το ίδιο αίτημα ενώπιον των δικαστηρίων, η υπόθεση τίθεται στο αρχείο από την Επιτροπή. Επίσης, η έκδοση απόφασης από την Επιτροπή δεν στερεί από τα εμπλεκόμενα μέρη το δικαίωμα να διεκδικήσουν την προστασία των έννομων συμφερόντων τους ενώπιον των δικαστηρίων (όπως προστέθηκε με το α. 52 παρ. 1 του ν. 4481/2017).	8. The commencement of the procedure before the Committee does not affect or prejudice the right of access to a tribunal for the same dispute. Where, however, the case has been brought to the courts by the same applicant and on the same grounds, the Committee shall archive the case. Also, the issuance of a decision by the Committee does not prevent the interested parties from exercising their right of access to a tribunal for the protection of their legitimate interests'.

Άρθρο 6, παράγραφος 2 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου Παν πρόσωπον κατηγορούμενον επί αδικήματι τεκμαίρεται ότι είναι αθώον μέχρι της νομίμου αποδείξεως της ενοχής του.	Article 6, paragraph 2 of the European Convention of Human Rights Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
Άρθρο 34 Νόμου 4624/2019, παρ. 1-3, Δικαίωμα διαγραφής 1. Αν η διαγραφή σε περίπτωση μη αυτοματοποιημένης επεξεργασίας λόγω της ιδιαίτερης φύσης της αποθήκευσης δεν είναι δυνατή ή είναι δυνατή μόνο με δυσανάλογα μεγάλη προσπάθεια και το συμφέρον του υποκειμένου των δεδομένων για τη διαγραφή δεν θεωρείται σημαντικό, δεν υφίσταται το δικαίωμα του υποκειμένου και η υποχρέωση του υπεύθυνου επεξεργασίας να διαγράψει τα δεδομένα προσωπικού χαρακτήρα σύμφωνα με το άρθρο 17 παράγραφος 1 του ΓΚΠΔ, εκτός των εξαιρέσεων που αναφέρονται στο άρθρο 17 παράγραφος 3 του ΓΚΠΔ. Στην περίπτωση αυτή, η διαγραφή αντικαθίσταται από τον περιορισμό της επεξεργασίας σύμφωνα με το άρθρο 18 του ΓΚΠΔ. Τα ανωτέρω εδάφια δεν εφαρμόζονται, εάν τα δεδομένα προσωπικού χαρακτήρα έχουν υποστεί παράνομη επεξεργασία. 2. Εκτός από το άρθρο 18 παράγραφος 1 στοιχεία β) και γ) του ΓΚΠΔ, το πρώτο και δεύτερο εδάφιο της προηγούμενης παραγράφου εφαρμόζονται αναλόγως στην περίπτωση του άρθρου 17 παράγραφος 1 στοιχεία α) και δ) του ΓΚΠΔ, στον βαθμό που ο υπεύθυνος επεξεργασίας έχει λόγους να πιστεύει ότι η διαγραφή θα ήταν επιζήμια για τα έννομα συμφέροντα του υποκειμένου των δεδομένων προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων σχετικά με τον περιορισμό της επεξεργασίας, εάν η ενημέρωση αυτή δεν είναι αδύνατη ή δεν συνεπάγεται δυσανάλογη προσπάθεια. 3. Εκτός από το άρθρο 17 παράγραφος 3 στοιχείο β) του ΓΚΠΔ, η παράγραφος 1 εφαρμόζεται αναλόγως στην περίπτωση του άρθρου 17 παράγραφος 1 στοιχείο α) του ΓΚΠΔ, εάν η διαγραφή θα ερχόταν σε	Article 34 of the Greek Law No. 4624/2019, par. 1-3, Right to delete If deletion in the event of manual processing due to the special nature of the storage is not possible or is possible only with a disproportionate amount of effort and the data subject's interest in the deletion is not considered significant, the right of the subject and the obligation for the controller shall not exist to delete personal data in accordance with Article 17 (1) of the GDPR, except for the exceptions referred to in Article 17 (3) of the GDPR. In this case, the deletion shall be replaced by the restriction of processing in accordance with Article 18 of the GDPR. The above paragraphs shall not apply if the personal data has been illegally processed. 2. In addition to Article 18 (1) (b) and (c) of the GDPR, the first and second subparagraphs of the preceding paragraph shall apply mutatis mutandis to Article 17 (1) (a) and (d) of the GDPR, to the extent that the controller has reason to believe that the deletion would be prejudicial to the legitimate interests of the data subject. The controller shall inform the data subject of the restriction of the processing if such updating is not impossible or does not entail a disproportionate effort. 3. In addition to Article 17 (3) (b) of the GDPR, paragraph 1 shall apply mutatis mutandis to Article 17 (1) (a) of the GDPR if the deletion would conflict with legal or contractual retention periods.

σύγκρουση με τις νόμιμες ή συμβατικές περιόδους διατήρησης.	
Άρθρο 35 του Νόμου 4624/2019, παρ.1, Δικαίωμα εναντίωσης Το δικαίωμα εναντίωσης σύμφωνα με το άρθρο 21 παράγραφος 1 του ΓΚΠΔ δεν εφαρμόζεται έναντι δημόσιου φορέα, εάν υπάρχει επιτακτικό δημόσιο συμφέρον για την επεξεργασία, το οποίο υπερτερεί των συμφερόντων του υποκειμένου των δεδομένων ή διάταξη νόμου υποχρεώνει τη διενέργεια της επεξεργασίας.	Article 35 of the Greek Law No. 4624/2019, par. 1, Right to object The right of opposition under Article 21 (1) of the GDPR does not apply to a public body if there is an overriding public interest in the processing which goes beyond the interests of the data subject or a provision of law obliges the processing to take place.
Άρθρο 14 του Προεδρικού Διατάγματος με αριθμ.131/2003, παρ.1-2, Απουσία γενικής υποχρέωσης ελέγχου των παρόχων 1. Οι φορείς παροχής υπηρεσιών δεν έχουν, για την παροχή υπηρεσιών που αναφέρονται στα «άρθρα 11,12, και 13» του παρόντος γενική υποχρέωση ελέγχου των πληροφοριών που μεταδίδουν ή αποθηκεύουν ούτε γενική υποχρέωση δραστήριας αναζήτησης γεγονότων ή περιστάσεων που δείχνουν ότι πρόκειται για παράνομες δραστηριότητες. 2. Χωρίς να παραβιάζονται οι διατάξεις περί προστασίας του απορρήτου και των προσωπικών δεδομένων, οι φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας είναι υποχρεωμένοι να ενημερώνουν πάραυτα τις αρμόδιες κρατικές αρχές για τυχόν υπόνοιες περί χορηγουμένων παράνομων πληροφοριών ή δραστηριοτήτων που επιχειρούν αποδέκτες των υπηρεσιών τους, και να ανακοινώνουν στις αρμόδιες αρχές κατ`αίτησή τους πληροφορίες που διευκολύνουντην εντόπιση αποδεκτών των υπηρεσιών τους με τους οποίους έχουν συμφωνίες αποθήκευσης.	Article 14 of the Greek Presidential Decree No. 131/2003, par.1-2, Absence of a general liability to exercise control of the service providers 1. Service providers have no general obligation to control the information transmitted or stored for the purpose of providing the services referred to in 'Articles 11, 12 and 13', nor is there a general obligation to actively seek out facts or circumstances which indicate that they are unlawful activities. 2. Without prejudice to the provisions on the protection of privacy and personal data, information society service providers are obliged to immediately inform the competent state authorities of any suspicion of unlawful information or activities being attempted by recipients of their services, and communicate to the competent authorities at their request information facilitating the identification of recipients of their services with whom they have storage agreements.
Άρθρο 11 του Προεδρικού Διατάγματος με αριθμ. 131/2003, παρ. 1-3, Ευθύνη μεσαζόντων παροχής υπηρεσιών - Απλή μετάδοση	Article 11 of the Greek Presidential Decree No. 131/2003, par. 1-3, The liability of the intermediaries services providers – The simple transmission

1. Σε περίπτωση παροχής μιας υπηρεσίας της κοινωνίας της πληροφορίας συνισταμένης στη μετάδοση πληροφοριών που παρέχει ο αποδέκτης της υπηρεσίας σε ένα δίκτυο επικοινωνιών ή στην παροχή πρόσβασης στο δίκτυο επικοινωνιών, δεν υφίσταται ευθύνη του φορέα παροχής υπηρεσιών όσον αφορά τις μεταδιδόμενες πληροφορίες, υπό τους όρους ότι ο φορέας παροχής υπηρεσιών: α) δεν αποτελεί την αφετηρία της μετάδοσης των πληροφοριών, β) δεν επιλέγει τον αποδέκτη της μετάδοσης και γ) δεν επιλέγει και δεν τροποποιεί τις μεταδιδόμενες πληροφορίες.	1. Where an information society service is provided consisting in the transmission of information provided by the recipient of the service to a communications network or in providing access to the communications network, the service provider shall not be liable for the information transmitted, provided that the service provider: (a) is not the starting point for the transmission of information; (b) does not select the recipient of the transmission; and (c) does not select or modify the information transmitted.
2. Οι δραστηριότητες μετάδοσης και παροχής πρόσβασης που αναφέρονται στην παράγραφο 1 περιλαμβάνουν την αυτόματη, ενδιάμεση και προσωρινή αποθήκευση των μεταδιδομένων πληροφοριών, στο βαθμό που η αποθήκευση εξυπηρετεί αποκλειστικά την πραγματοποίηση της μετάδοσης στο δίκτυο επικοινωνιών και η διάρκειά της δεν υπερβαίνει το χρόνο που είναι ευλόγως απαραίτητος για τη μετάδοση.	2. The transmission and access activities referred to in paragraph 1 shall include the automatic, intermediate and temporary storage of transmitted information insofar as the storage is for the sole purpose of transmitting to the communications network and its duration does not exceed a reasonable time necessary for transmission.
3. Το παρόν άρθρο δεν θίγει τη δυνατότητα να επιβληθεί δικαστικά ή διοικητικά στον φορέα παροχής υπηρεσιών η παύση ή η πρόληψη της παράβασης.	3. This Article shall be without prejudice to the possibility for the service provider to bring an action to cease or prevent an infringement.
Άρθρο 12 του Προεδρικού Διατάγματος με αριθμ. 131/2003, παρ. 1-2, Αποθήκευση σε κρυφή μνήμη	Article 12 of the Greek Presidential Decree No. 131/2003, par. 1-2, The Cache storage
1. Σε περίπτωση παροχής μιας υπηρεσίας της κοινωνίας της πληροφορίας, η οποία συνίσταται στη μετάδοση πληροφοριών που παρέχει ένας αποδέκτης υπηρεσίας σε ένα δίκτυο επικοινωνιών, δεν υφίσταται ευθύνη του φορέα παροχής της υπηρεσίας, όσον αφορά την αυτόματη, ενδιάμεση και προσωρινή αποθήκευση των πληροφοριών, η οποία γίνεται με αποκλειστικό σκοπό να καταστεί αποτελεσματικότερη η μεταγενέστερη μετάδοση των πληροφοριών προς άλλους αποδέκτες της υπηρεσίας, κατ` αίτησή τους, υπό τους όρους ότι ο φορέας παροχής υπηρεσιών: (α) δεν τροποποιεί τις πληροφορίες,	1. In the event of the provision of an information society service consisting in the transmission of information provided by a recipient of service to a communications network, the service provider shall not be responsible for the automatic, intermediate and temporary storage of information, which is for the sole purpose of making the subsequent transmission of the information to other recipients of the service more effective upon request, provided that the service provider: (a) does not modify the information;

(β) τηρεί τους όρους πρόσβασης στις πληροφορίες, (γ) τηρεί τους κανόνες που αφορούν την ενημέρωση των πληροφοριών, οι οποίοι καθορίζονται κατά ευρέως αναγνωρισμένο τρόπο και χρησιμοποιούνται από τον κλάδο, (δ) δεν παρεμποδίζει τη νόμιμη χρήση της τεχνολογίας, η οποία αναγνωρίζεται και χρησιμοποιείται ευρέως από τον κλάδο, προκειμένου να αποκτήσει δεδομένα σχετικά με τη χρησιμοποίηση των πληροφοριών, και (ε) ενεργεί άμεσα προκειμένου να αποσύρει τις πληροφορίες που αποθήκευσε ή να καταστήσει την πρόσβαση σε αυτές αδύνατη, μόλις αντιληφθεί ότι οι πληροφορίες έχουν αποσυρθεί από το σημείο του δικτύου στο οποίο βρίσκονταν αρχικά ή η πρόσβαση στις πληροφορίες κατέστη αδύνατη ή μια δικαστική ή διοικητική αρχή διέταξε την απόσυρση των πληροφοριών ή απαγόρευσε την πρόσβαση σε αυτές.	(b) comply with the conditions of access to information; (c) adhere to the rules for updating information, which are widely recognised and used by the industry; (d) does not impede the legitimate use of technology, which is widely recognised and used by the industry, in order to obtain data on the use of information; and (e) act immediately to retrieve the information stored or make it impossible to access as soon as it realises that the information has been withdrawn from the network point where it was originally located or that access to the information has become impossible or a judicial or administrative authority ordered the information to be withdrawn or denied access.
Το παρόν άρθρο δεν θίγει την δυνατότητα να επιβληθεί δικαστικά ή διοικητικά στο φορέα παροχής υπηρεσιών η παύση ή η πρόληψη της παράβασης.	2. This Article shall be without prejudice to the judicial or administrative authority imposing a cessation or prevention of the infringement.
Άρθρο 13 του Προεδρικού Διατάγματος με αριθμ. 131/2003, παρ. 1-3, Φιλοξενία 1. Σε περίπτωση παροχής μιας υπηρεσίας της κοινωνίας της πληροφορίας συνισταμένης στην αποθήκευση πληροφοριών παρεχομένων από ένα αποδέκτη υπηρεσίας, δεν υφίσταται ευθύνη του φορέα παροχής της υπηρεσίας για τις πληροφορίες που αποθηκεύονται μετά από αίτηση αποδέκτη της υπηρεσίας, υπό τους όρους ότι: (α) ο φορέας παροχής της υπηρεσίας δεν γνωρίζει πραγματικά ότι πρόκειται για παράνομη δραστηριότητα ή πληροφορία και ότι, σε ό, τι αφορά αξιώσεις αποζημιώσεως, δεν γνωρίζει τα γεγονότα ή τις περιστάσεις από τις οποίες προκύπτει η παράνομη δραστηριότητα ή πληροφορία, ή (β) ο φορέας παροχής της υπηρεσίας, μόλις αντιληφθεί τα προαναφερθέντα, αποσύρει	Article 13 of the Greek Presidential Decree No. 131/2003, par. 1-3, The hospitality 1. Where an information society service is provided consisting of storing information provided by a recipient of the service, the service provider shall not be responsible for the information stored at the request of the recipient of the service, provided that: (a) the service provider does not really know that it is an illegal activity or information and that, as far as compensation claims are concerned, he is not aware of the facts or circumstances resulting from the illegal activity or information, or (b) the service provider, as soon as it is aware of the above, rapidly withdraws the

ταχέως τις πληροφορίες ή καθιστά την πρόσβαση σε αυτές αδύνατη. 2. Η παράγραφος 1 δεν εφαρμόζεται όταν ο αποδέκτης της υπηρεσίας ενεργεί υπό την εξουσία ή υπό τον έλεγχο του φορέα παροχής της υπηρεσίας. 3. Το παρόν άρθρο δεν θίγει τη δυνατότητα να επιβληθεί δικαστικά ή διοικητικά στο φορέα παροχής υπηρεσιών η παύση ή η πρόληψη της παράβασης.	information or makes it impossible to access. 2. Paragraph 1 shall not apply where the recipient of the service is acting under the authority or control of the service provider. 3. This Article shall be without prejudice to the possibility for the service provider to bring an action to cease or prevent the infringement.
Άρθρο 37 του Νόμου 4070/2012, παρ.1, Ασφάλεια και ακεραιότητα δικτύων και υπηρεσιών 1. Οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών. Τα μέτρα αυτά, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τον υφιστάμενο κίνδυνο. Οι επιχειρήσεις αυτές λαμβάνουν ιδίως μέτρα για την αποτροπή και ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφαλείας που επηρεάζουν τους χρήστες και τα διασυνδεμένα δίκτυα.	Article 37 of the Greek Law No. 4070/2012, par. 1, Security and integrity of networks and services 1. Undertakings providing public communications networks or publicly available electronic communications services shall take appropriate technical and organisational measures to adequately manage the security risk of networks and services. These measures, taking into account the latest technical possibilities, should ensure a level of safety commensurate with the existing risk. These undertakings shall, in particular, take measures to prevent and minimise the impact of security incidents affecting users and interconnected networks.
Άρθρο 60 Νόμου 4624/2019, παρ. 1-7, Εκτελών την επεξεργασία 1. Όταν η επεξεργασία διενεργείται για λογαριασμό υπεύθυνου επεξεργασίας, αυτός μεριμνά για την τήρηση των υποχρεώσεων που απορρέουν από τον παρόντα νόμο και από άλλες διατάξεις σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Το δικαίωμα του υποκειμένου για ενημέρωση, διόρθωση, διαγραφή και περιορισμό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, καθώς και η αξίωση	Article 60 of the Greek Law No. 4624/2019, par. 1-7, The processor 1. Where processing is carried out on behalf of a controller, he shall ensure that his obligations under this Act and other provisions concerning the protection of personal data are complied with. The right of the subject to update, correct, delete and limit the processing of personal data, as well as to claim compensation in this case, shall be exercised against the controller.

αποζημίωσης στην περίπτωση αυτή ασκούνται έναντι του υπεύθυνου επεξεργασίας.	
2. Ο υπεύθυνος επεξεργασίας επιτρέπεται να αναθέσει την επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνο σε εκτελούντες την επεξεργασία, οι οποίοι εξασφαλίζουν με κατάλληλα τεχνικά και οργανωτικά μέτρα ότι η επεξεργασία διενεργείται σύμφωνα με τον νόμο και ότι διασφαλίζεται η προστασία των δικαιωμάτων των υποκειμένων επεξεργασίας.	2. The controller may delegate the processing of personal data only to processors who ensure by appropriate technical and organisational measures that the processing is carried out in accordance with the law and that the rights of the processors are protected.
3. Η επεξεργασία μέσω εκτελούντος την επεξεργασία πρέπει να βασίζεται σε σύμβαση ή άλλη νομική πράξη που συνδέει τον εκτελούντα την επεξεργασία με τον υπεύθυνο επεξεργασίας, η οποία καθορίζει το αντικείμενο, τη διάρκεια, τη φύση και το σκοπό της επεξεργασίας, τη φύση των δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες των υποκειμένων και τα δικαιώματα και τις υποχρεώσεις του υπεύθυνου προσώπου. Η σύμβαση ή άλλη νομική πράξη προβλέπει ιδίως ότι ο εκτελών την επεξεργασία:	3. Processing by the processor shall be based on a contract or other legal act linking the processor with the controller, which specifies the object, duration, nature and purpose of the processing, the nature of the personal data nature, categories of subjects and rights and obligations of the responsible person. The contract or other legal instrument provides in particular that the contractor shall:
α) ενεργεί μόνο κατ` εντολή και σύμφωνα με τις οδηγίες του υπεύθυνου επεξεργασίας, εάν ο εκτελών την επεξεργασία θεωρεί ότι μια εντολή είναι παράνομη, πρέπει να ενημερώσει τον υπεύθυνο επεξεργασίας χωρίς καθυστέρηση·	(a) acts only on the instructions and in accordance with the instructions of the controller, if the processor considers that a command is illegal, he must inform the controller without delay;
β) εγγυάται ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα είναι υποχρεωμένα να τηρούν την εμπιστευτικότητα, στο μέτρο που αυτά δεν υπόκεινται σε καμία εύλογη νομική υποχρέωση διατήρησης του απορρήτου·	(b) it guarantees that persons authorised to process personal data are obliged to respect confidentiality, in so far as they are not subject to any reasonable legal obligation of confidentiality;
γ) βοηθά με τα κατάλληλα μέσα τον υπεύθυνο επεξεργασίας για τη διασφάλιση των δικαιωμάτων του υποκειμένου των δεδομένων·	(c) assist the controller by appropriate means to ensure the rights of the data subject;
δ) μετά την ολοκλήρωση της παροχής των υπηρεσιών επεξεργασίας κατά την κρίση του υπεύθυνου επεξεργασίας επιστρέφει ή διαγράφει όλα τα προσωπικά δεδομένα και καταστρέφει τα υπάρχοντα αντίγραφα, εκτός	(d) upon completion of the provision of processing services at the discretion of the controller, it returns or deletes all personal data and destroys existing copies unless there is a legal obligation to store the data;

εάν υπάρχει νομική υποχρέωση αποθήκευσης των δεδομένων·	
ε) παρέχει στον υπεύθυνο επεξεργασίας όλες τις απαραίτητες πληροφορίες, ιδίως τις δημιουργηθείσες καταχωρίσεις σύμφωνα με το άρθρο 74, ως απόδειξη συμμόρφωσης με τις υποχρεώσεις του·	(e) provide the controller with all necessary information, in particular alerts made under Article 74, as proof of compliance with its obligations;
στ) επιτρέπει και συμβάλλει στη διενέργεια ελέγχων που διενεργεί ο υπεύθυνος επεξεργασίας ή ο εξουσιοδοτημένος από αυτόν ελεγκτής·	(f) authorises and contributes to audits carried out by the controller or the auditor authorised by him;
ζ) λαμβάνει όλα τα αναγκαία μέτρα σύμφωνα με το άρθρο 62·	(g) take all necessary measures in accordance with Article 62;
η) λαμβανομένης υπόψη της φύσης της επεξεργασίας και των πληροφοριών που έχει στη διάθεσή του, βοηθά τον υπεύθυνο επεξεργασίας για την τήρηση των υποχρεώσεων που ορίζονται στα άρθρα 62 έως 65 και 67.	(h) having regard to the nature of the processing and the information at its disposal, assist the controller in complying with the obligations laid down in Articles 62 to 65 and 67.
4. Σε περίπτωση που ο εκτελών την επεξεργασία αναθέτει σε άλλον εκτελούντα την επεξεργασία, πρέπει να του επιβάλει τις ίδιες υποχρεώσεις σύμφωνα με τη σύμβασή του με τον υπεύθυνο επεξεργασίας, σύμφωνα με την παράγραφο 3, η οποία ισχύει και για τον ίδιο, εκτός εάν οι υποχρεώσεις αυτές δεσμεύουν ήδη τον άλλον εκτελούντα την επεξεργασία βάσει άλλων διατάξεων.	4. If the contractor assigns the processor to another contractor, he must impose the same obligations under his contract with the contractor in accordance with paragraph 3, which also applies to him, unless the contractor these obligations already bind the other party to the processing under other provisions.
5. Ο εκτελών την επεξεργασία δύναται να αναθέσει την επεξεργασία σε άλλον, μόνο κατόπιν προηγούμενης έγγραφης άδειας του υπεύθυνου επεξεργασίας. Εάν ο υπεύθυνος επεξεργασίας έχει χορηγήσει στον εκτελούντα την επεξεργασία γενική άδεια για τη συμμετοχή και άλλου εκτελούντος την επεξεργασία, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για τυχόν αλλαγές, στις οποίες σκοπεύει να προβεί και που αφορούν την ενδεχόμενη συμπλήρωση ή αντικατάσταση άλλων εκτελούντων την επεξεργασία. Ο υπεύθυνος επεξεργασίας δύναται στην περίπτωση αυτή να αρνηθεί αυτές τις αλλαγές.	5. The processor may delegate the process to another only with the prior written permission of the controller. If the controller has granted the processor a general authorisation to participate and another processor, the processor shall inform the processor of any changes he intends to make to the completion or replacement of other processors by the processor. The controller may then refuse these changes.

6. Η σύμβαση που αναφέρεται στην παράγραφο 3 πρέπει να είναι έγγραφη ή ηλεκτρονική.	6. The contract referred to in paragraph 3 must be in writing or electronic.
7. Ο εκτελών την επεξεργασία που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας κατά παράβαση του παρόντος άρθρου θεωρείται υπεύθυνος επεξεργασίας.	7. The operator who determines the purposes and means of processing in breach of this Article shall be deemed to be the controller.
Άρθρο 38 Νόμου 4624/2019, παρ. 1-5, Ποινικές κυρώσεις	Article 38 of the Greek Law No. 4624/2019, par. 1-5, Criminal sanctions
1. Όποιος, χωρίς δικαίωμα: α) επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών· β) τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει, τιμωρείται με φυλάκιση μέχρι ενός (1) έτους, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.	1. Whoever, without right: a) intervenes in any way in a system of archiving personal data, and by this act becomes aware of this data; b) copies, removes, alters, damages, collects, registers, organises, structures, stores, adapts, modifies, recovers, searches for information, correlates, combines, restricts, deletes, destroys, is punished with imprisonment of up to one (1) year, if the act is not more severely punished by another provision.
2. Όποιος χρησιμοποιεί, μεταδίδει, διαδίδει, κοινολογεί με διαβίβαση, διαθέτει, ανακοινώνει ή καθιστά προσιτά σε μη δικαιούμενα πρόσωπα δεδομένα προσωπικού χαρακτήρα, τα οποία απέκτησε σύμφωνα με την περίπτωση α΄ της παραγράφου 1 ή επιτρέπει σε μη δικαιούμενα πρόσωπα να λάβουν γνώση των δεδομένων αυτών, τιμωρείται με φυλάκιση, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.	2. Whoever uses, transmits, disseminates, communicates by transmission, has, announces or makes available to unauthorised persons personal data, which he acquired in accordance with indent a of paragraph 1 or allows unauthorised persons to become aware of the data of these, shall be punishable by imprisonment if the act is not more severely punished by another provision.
3. Εάν η πράξη της παραγράφου 2 αφορά ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα του άρθρου 9 παράγραφος 1 του ΓΚΠΔ ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα ή τα σχετικά με αυτά μέτρα ασφαλείας του άρθρου 10 του ΓΚΠΔ, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή έως εκατό χιλιάδες (100.000) ευρώ, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη.	3. If the act referred to in paragraph 2 concerns specific categories of personal data referred to in Article 9 (1) of the GDPR or data relating to criminal convictions and offenses or related security measures referred to in Article 10 of the GDPR, the offender shall be punished by imprisonment of at least one (1) year and a fine of up to one hundred thousand (100,000) euros, if the transaction is not more severely punished by another provision.

4. Με κάθειρξη μέχρι δέκα (10) ετών τιμωρείται ο υπαίτιος των πράξεων των προηγούμενων παραγράφων, εάν είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να προκαλέσει περιουσιακή ζημία σε άλλον ή να βλάψει άλλον και το συνολικό όφελος ή η συνολική ζημία υπερβαίνει το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ.	4. A person convicted of the acts referred to in the preceding paragraphs shall be punished by imprisonment of up to ten (10) years, if he intended to offer himself or another illegal property or to cause property damage to another or to harm another and the total benefit or total damage exceeds the amount of one hundred and twenty thousand (120,000) euros.
5. Εάν από τις πράξεις των παραγράφων 1 έως και 3 προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή έως τριακόσιες χιλιάδες (300.000) ευρώ.	5. If the acts referred to in paragraphs 1 to 3 endanger the free functioning of the democratic state or national security, imprisonment and a fine of up to three hundred thousand (300,000) euros shall be imposed.
Άρθρο 66 Νόμου 2121/1993, παρ.1, Ποινικές κυρώσεις 1. Τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή 2.900 15.000 ευρώ όποιος χωρίς δικαίωμα και κατά παράβαση των διατάξεων του παρόντος νόμου ή διατάξεων των κυρωμένων με νόμο πολυμερών διεθνών συμβάσεων για την Προστασία της πνευματικής ιδιοκτησίας εγγράφει έργα ή αντίτυπα, αναπαράγει αυτά άμεσα ή έμμεσα, προσωρινά ή μόνιμα, με οποιαδήποτε μορφή, εν όλω ή εν μέρει, μεταφράζει, διασκευάζει, προσαρμόζει ή μετατρέπει αυτά, προβαίνει σε διανομή αυτών στο κοινό με πώληση ή με άλλους τρόπους ή κατέχει με σκοπό διανομής, εκμισθώνει, εκτελεί δημόσια, μεταδίδει ραδιοτηλεοπτικά κατά οποιονδήποτε τρόπο, παρουσιάζει στο κοινό έργα ή αντίτυπα με οποιονδήποτε τρόπο, εισάγει αντίτυπα του έργου που παρήχθησαν παράνομα στο εξωτερικό χωρίς τη συναίνεση του δημιουργού και γενικά εκμεταλλεύεται έργα, αντίγραφα ή αντίτυπα που είναι αντικείμενο πνευματικής ιδιοκτησίας ή προσβάλλει το Ηθικό δικαίωμα του πνευματικού δημιουργού να αποφασίζει για τη δημοσίευση του έργου στο κοινό, καθώς και να παρουσιάζει αυτό αναλλοίωτο χωρίς προσθήκες ή περικοπές. (άρθρο 8 παρ. 1 Οδηγίας 2001/29).	Article 66 of the Greek Law No. 2121/1993, par. 1, Criminal Sanctions 1. Sentenced to imprisonment of at least one year and a fine of 2,900 EUR 15,000, who without any right and in breach of the provisions of this Act or of the provisions of multilateral international agreements for the protection of intellectual property, records works or copies, reproduces them directly or indirectly; , temporarily or permanently, in any form, in whole or in part, translate, adapt, adapt or modify them, distribute them to the public by sale or other means, or own, for distribution, rent, publicly broadcasts, broadcasts in any way, presents to the public works or copies in any way, imports copies of the work that were illegally produced abroad without the consent of the creator, and generally exploits works, copies, or copyrighted works the right of the intellectual author to decide on the work to be published and to present it unaltered without any additions or cuts. (Article 8 (1) of Directive 2001/29).

Άρθρο 348Α του Νόμου 4619/2019, παρ. 1-6,	Article 348A of the Greek Law No. 4619/2019, par. 1-6,
Πορνογραφία ανηλίκων	Minors Pornography
1. Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή.	1. Anyone intentionally producing, distributing, publishing, displaying, importing or exporting from the Territory, transmitting, offering, selling or otherwise disposing of, purchasing, purchasing, acquiring or possessing child pornography material or disseminating or transmitting information about perpetration of the above offenses, is punishable by imprisonment of at least one year and a fine.
2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.	2. Anyone who intentionally produces, offers, sells or otherwise disposes of, distributes, transmits, purchases, supplies or owns child pornography or disseminates information about the commission of the above acts through information systems, is punishable by imprisonment of at least two years, and fine.
3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων συνιστά η αναπαράσταση ή η πραγματική ή η εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα των γεννητικών οργάνων ή του σώματος εν γένει του ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής γενετήσιας πράξης που διενεργείται από ή με ανήλικο.	3. Child pornography material, within the meaning of the preceding paragraphs, is the representation or actual or virtual imprinting on an electronic or other physical carrier of the minor's genitals or body in a manner which is manifestly causing sexual arousal and actual or virtual sexual act performed by or with a minor.
4. Οι πράξεις των παραγράφων 1 και 2 τιμωρούνται με κάθειρξη έως δέκα έτη και χρηματική ποινή: α. αν τελέσθηκαν κατ` επάγγελμα, β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή της σωματικής δυσλειτουργίας, λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος ή αν η παραγωγή του υλικού της παιδικής πορνογραφίας εξέθεσε τη ζωή του ανηλίκου σε σοβαρό κίνδυνο και	4. The acts referred to in paragraphs 1 and 2 shall be punishable by up to ten years of imprisonment and a fine of: a. if done professionally, b. whether the production of child pornography material is related to the exploitation of need, mental or mental illness or physical impairment, due to an organic juvenile disease, or to the exercise or threat of abuse of a minor or to the use of a minor who has not reached the tenth fifth year or if the production of child pornography material puts the minor's life in serious danger; and

γ. αν δράστης της παραγωγής του υλικού παιδικής πορνογραφίας είναι πρόσωπο στο οποίο έχουν εμπιστευθεί ανήλικο για να τον επιβλέπει ή να τον φυλάσσει, έστω και προσωρινά.	c. if the perpetrator of the production of child pornography material is a person they have entrusted with a minor to supervise or guard, even temporarily.
5. Αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δωδέκατο έτος της ηλικίας του, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή. Η ίδια ποινή επιβάλλεται αν η πράξη των περιπτώσεων β` και γ` της προηγούμενης παραγράφου είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται κάθειρξη ισόβια ή πρόσκαιρη τουλάχιστον δέκα ετών και χρηματική ποινή.	5. If the production of child pornography material is linked to the use of a minor who has not reached the age of twelve years, a minimum of 10 years' imprisonment and a fine shall be imposed. The same penalty applies if the act of cases b) and c) of the previous paragraph resulted in serious bodily harm, and if it resulted in death, life imprisonment of at least ten years and a fine of at least ten years.
6. Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή.	6. Anyone who knowingly gains access to child pornography through information systems is punishable by up to three years in prison or a fine.
Αρ. 1(1) του ν. 2121/1993 περί πνευματικής ιδιοκτησίας Οι πνευματικοί δημιουργοί, με τη δημιουργία του έργου, αποκτούν πάνω ϋ αυτό πνευματική ιδιοκτησία, που περιλαμβάνει, ως αποκλειστικά και απόλυτα δικαιώματα, το δικαίωμα της εκμετάλλευσης του έργου (περιουσιακό δικαίωμα) και το δικαίωμα της προστασίας του προσωπικού τους δεσμού προς αυτό (ηθικό δικαίωμα).	Art. 1(1) of the Law 2121/1993 on Intellectual Property Creators, by creating the work, acquire intellectual property on it, which includes, as exclusive and absolute rights, the right to exploit the work (property right) and the right of protection of their personal connection to it (moral right).
Αρ. 2(2α) του ν. 2121/1993 Αντικείμενο προστασίας είναι και οι βάσεις δεδομένων οι οποίες λόγω της επιλογής ή διευθέτησης του περιεχομένου τους αποτελούν πνευματικά δημιουργήματα. Η προστασία αυτή δεν εκτείνεται στο περιεχόμενο των βάσεων δεδομένων και δεν θίγει κανένα από τα δικαιώματα που υφίστανται στο περιεχόμενο αυτό.	Article 2(2a) of law 2121/1993 Subject-matter of protection comprise also the databases which, due to the choice or settlement of their content, are considered intellectual creations. This protection does not extend to the content of the databases and does not affect any of the rights in that content.

Αρ. 183 του Ποινικού Κώδικα (Διέγερση) Όποιος δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου προκαλεί ή διεγείρει σε απείθεια κατά των νόμων ή των διαταγμάτων ή εναντίον άλλων νόμιμων διαταγών της αρχής, τιμωρείται με φυλάκιση έως ένα έτος ή με χρηματική ποινή.	Art. 183 of the Criminal Code (Incitement to Disobedience) Anyone who, in any way or via the Internet, causes or incites defiance against the laws or orders or against other legal orders is punishable with up to one year or a fine.
Αρ. 184(1) του Ποινικού Κώδικα (Διέγερση σε διάπραξη εγκλημάτων, βιαιοπραγίες ή διχόνοια) Όποιος δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου προκαλεί ή διεγείρει σε διάπραξη πλημμελήματος ή κακουργήματος και έτσι εκθέτει σε κίνδυνο τη δημόσια τάξη τιμωρείται με φυλάκιση έως ένα έτος ή με χρηματική ποινή.	Article 184(1) of the Criminal Code (Incitement to commit crimes, violence or discord) Anyone who is publicly, in any way or via the Internet, causes or incites a misdemeanor or felony and thus endangers public order is punishable with imprisonment of up to one year or with a penalty fee.
Αρ. 184(2) του Ποινικού Κώδικα Με φυλάκιση έως τρία έτη ή χρηματική ποινή τιμωρείται η πράξη της προηγούμενης παραγράφου αν με αυτήν επιχειρείται η τέλεση βιαιοπραγιών κατά ομάδας ή προσώπου που προσδιορίζεται με βάση τα χαρακτηριστικά της φυλής, το χρώμα, την εθνική ή εθνοτική καταγωγή, τις γενεαλογικές καταβολές, τη θρησκεία, την αναπηρία, το γενετήσιο προσανατολισμό, την ταυτότητα ή τα χαρακτηριστικά φύλου.	Article 184(2) of the Criminal Code Imprisonment of up to three years or a fine of imprisonment shall be punishable by the act of paragraph whether it is attempted to commit violence against a group of person identified on the basis of the characteristics of the race, colour, ethnic or ethnic origin, the characteristics of the genealogical origins, religion, disability, sexual orientation, identity or gender characteristics.
Αρ. 187(6) του Ποινικού Κώδικα Όποιος δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου απειλεί με τέλεση τρομοκρατικής πράξης ή προκαλεί ή διεγείρει σε διάπραξή της και έτσι εκθέτει σε κίνδυνο τη δημόσια τάξη τιμωρείται με φυλάκιση.	Article 187(6) of the Criminal Code Anyone who is publicly, in any way or via the Internet, threatens to commit terrorist acts or provokes or stimulates its commitment and thus exposes public order to a risk is punishable by imprisonment.
Αρ. 362 του Ποινικού Κώδικα (Δυσφήμηση) Όποιος με οποιονδήποτε τρόπο ενώπιον τρίτου ισχυρίζεται ή διαδίδει για κάποιον άλλον γεγονός που μπορεί να βλάψει την τιμή ή την υπόληψή του τιμωρείται με φυλάκιση έως ένα έτος ή χρηματική ποινή. Αν η πράξη	Article 362 of the Criminal Code (Defamation) Anyone who in any way before a third party claims or disseminates before another any

τελέστηκε δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως τρία έτη ή χρηματική ποινή. Πρώην άρ. 362 του Ποινικού Κώδικα Όποιος με οποιονδήποτε τρόπο ενώπιον τρίτου ισχυρίζεται ή διαδίδει για κάποιον άλλον γεγονός που μπορεί να βλάψει την τιμή ή την υπόληψή του τιμωρείται με φυλάκιση μέχρι δύο ετών ή με χρηματική ποινή. Η χρηματική ποινή μπορεί να επιβληθεί και μαζί με την ποινή της φυλάκισης. Αρ. 57 του Αστικού Κώδικα Όποιος προσβάλλεται παράνομα στην προσωπικότητά του έχει δικαίωμα να απαιτήσει να αρθεί η προσβολή και να μην επαναληφθεί στο μέλλον. Αν η προσβολή αναφέρεται στην προσωπικότητα προσώπου που έχει πεθάνει, το δικαίωμα αυτό έχουν ο σύζυγος, οι κατιόντες, οι ανιόντες, οι αδελφοί και οι κληρονόμοι του από διαθήκη. Αξίωση αποζημίωσης σύμφωνα με τις διατάξεις για τις αδικοπραξίες δεν αποκλείεται.	event which may damage their honour or reputation is punishable by imprisonment of up to one year or penalty fee. If the act was committed publicly in any way or via the Internet, a punishment of up to three years or a penalty fee is imposed. Article 362 of the former Criminal Code Anyone who, in any way before a third party claims or disseminates for another event which may damage their honour or reputation is punishable by imprisonment of up to two years or by a fine.The penalty payment may also be imposed along with the sentence of theImprisonment. Article 57 of the Civil Code Anyone who is unlawfully offended in their personality has the right to demand that the insult be lifted and not repeated in the future. If the offence refers to the personality of a person who has died, that right is given by the spouse, descendants, ascendants, brothers and heirs according to their will. A claim of compensation in accordance with the provisions on torts is not excluded.
Αρ. 5(1) του Συντάγματος Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και πολιτική ζωή της Χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη. Αρ. 5Α του Συντάγματος 1. Καθένας έχει δικαίωμα στην πληροφόρηση, όπως νόμος ορίζει. Περιορισμοί στο δικαίωμα αυτό είναι δυνατόν να επιβληθούν με νόμο μόνο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων. 2. Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της	Article 5(1) of the Greek Constitution All persons shall have the right to develop freely their personality and to participate in the social, economic and political life of the country, insofar as they do not infringe the rights of others or violate the Constitution and the good usages. Article 5A of the Greek Constitution 1. All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties. 2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes

παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19.	an obligation of the State, always in observance of the guarantees of Articles 9, 9A and 19.
Αρ. 9Α του Συντάγματος	Article 9A of the Greek Constitution
Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.	All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law.
Αρ. 14(1) του Συντάγματος	Article 14(1) of the Greek Constitution
1. Καθένας μπορεί να εκφράζει και να διαδίδει προφορικά, γραπτά και δια του τύπου τους στοχασμούς του τηρώντας τους νόμους του Κράτους	Every person may express and propagate his thoughts orally, in writing and through the press in compliance with the laws of the State.
Αρ. 14(5) του Συντάγματος	Article 14(5) of the Greek Constitution
5. Καθένας ο οποίος θίγεται από ανακριβές δημοσίευμα ή εκπομπή έχει δικαίωμα απάντησης, το δε μέσο ενημέρωσης έχει αντιστοίχως υποχρέωση πλήρους και άμεσης επανόρθωσης. Καθένας ο οποίος θίγεται από υβριστικό ή δυσφημιστικό δημοσίευμα ή εκπομπή έχει, επίσης, δικαίωμα απάντησης, το δε μέσο ενημέρωσης έχει αντιστοίχως υποχρέωση άμεσης δημοσίευσης ή μετάδοσης της απάντησης. Νόμος ορίζει τον τρόπο με τον οποίο ασκείται το δικαίωμα απάντησης και διασφαλίζεται η πλήρης και άμεση επανόρθωση ή η δημοσίευση και μετάδοση της απάντησης.	Every person offended by an inaccurate publication or broadcast has the right to reply, and the information medium has a corresponding obligation for full and immediate redress. Every person offended by an insulting or defamatory publication or broadcast has also the right to reply, and the information medium
Αρ. 17(2) του Συντάγματος	Article 17(2) of the Greek Constitution
2. Κανένας δεν στερείται την ιδιοκτησία του, παρά μόνο για δημόσια ωφέλεια που έχει αποδειχθεί με τον προσήκοντα τρόπο [...]	No one shall be deprived of his property except for public benefit which must be duly proven [...]
Αρ. 19(1) του Συντάγματος	Article 19(1) of the Greek Constitution
1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα	Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guaranties under

απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.	which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes, shall be specified by law.
Αρ. 21(1) του Συντάγματος Η οικογένεια ως θεμέλιο της συντήρησης και προαγωγής του Έθνους, καθώς και ο γάμος, η μητρότητα και η παιδική ηλικία τελούν υπό την προστασία του Κράτους. Το Κράτος μεριμνά για τη διασφάλιση συνθηκών αξιοπρεπούς διαβίωσης όλων των πολιτών μέσω ενός συστήματος ελάχιστου εγγυημένου εισοδήματος, όπως νόμος ορίζει.	Article 21(1) of the Greek Constitution The family, being the cornerstone of the preservation and the advancement of the Nation, as well as marriage, motherhood and childhood, shall be under the protection of the State.
Αρ. 25(1), (3) του Συντάγματος 1. Τα δικαιώματα του ανθρώπου ως ατόμου και ως μέλους του κοινωνικού συνόλου και η αρχή του κοινωνικού κράτους δικαίου τελούν υπό την εγγύηση του Κράτους. Όλα τα κρατικά όργανα υποχρεούνται να διασφαλίζουν την ανεμπόδιστη και αποτελεσματική άσκησή τους. Τα δικαιώματα αυτά ισχύουν και στις σχέσεις μεταξύ ιδιωτών στις οποίες προσιδιάζουν. Οι κάθε είδους περιορισμοί που μπορούν κατά το Σύνταγμα να επιβληθούν στα δικαιώματα αυτά πρέπει να προβλέπονται είτε απευθείας από το Σύνταγμα είτε από το νόμο, εφόσον υπάρχει επιφύλαξη υπέρ αυτού και να σέβονται την αρχή της αναλογικότητας. 3. Η καταχρηστική άσκηση δικαιώματος δεν επιτρέπεται.	Article 25(1), (3) of the Greek Constitution 1. The rights of the human being as an individual and as a member of the society and the principle of the welfare state rule of law are guaranteed by the State. All agents of the State shall be obliged to ensure the unhindered and effective exercise thereof. These rights also apply to the relations between individuals to which they are appropriate. Restrictions of any kind which, according to the Constitution, may be imposed upon these rights, should be provided either directly by the Constitution or by statute, should a reservation exist in the latter's favour, and should respect the principle of proportionality. 3. The abusive exercise of rights is not permitted.
Αρ. 10 του ν. 4285/2014 Άρθρο 81Α Ρατσιστικό έγκλημα Εάν η πράξη τελείται από μίσος λόγω της φυλής, του χρώματος, της θρησκείας, των γενεαλογικών καταβολών, της εθνικής ή εθνοτικής καταγωγής, του σεξουαλικού προσανατολισμού, της ταυτότητας φύλου ή της αναπηρίας κατά του παθόντος, το κατώτερο όριο ποινής αυξάνεται ως εξής: Α) Σε περίπτωση πλημμελήματος, που το προβλεπόμενο όριο ποινής ορίζεται σε δέκα ημέρες έως ένα έτος φυλάκισης, το κατώτερο	Article10 of the Law 4285/2014 Art. 81A Racist crime If the act is committed by hatred on the grounds of race, colour, religion, genealogical payments, national or ethnic origin, sexual orientation, gender identity or disability against the victim, the lower penalty limit shall be increased as follows: (A) In the event of a misdemeanour, the prescribed penalty limit is set at ten days to one year in prison, the lower penalty limit

όριο ποινής αυξάνεται κατά έξι μήνες και κατά ένα έτος στις λοιπές περιπτώσεις πλημμελημάτων. Β) Σε περίπτωση κακουργήματος, που το προβλεπόμενο όριο ποινής ορίζεται σε πέντε έως δέκα έτη κάθειρξης, το κατώτερο όριο ποινής αυξάνεται κατά δύο έτη και κατά τρία έτη στις λοιπές περιπτώσεις κακουργημάτων.	shall be increased by six months and by one year in other cases of misdemeanours. B) In the case of a felony, the prescribed penalty limit is set at five to ten years of imprisonment, the lower penalty limit shall be increased by two years and by three years in other cases of felonies.
Αρ. 21 του ν. 4356/2015 Άρθρο 81Α Έγκλημα με ρατσιστικά χαρακτηριστικά Εάν από τις περιστάσεις προκύπτει ότι έχει τελεστεί έγκλημα κατά παθόντος, η επιλογή του οποίου έγινε λόγω των χαρακτηριστικών φυλής, χρώματος, εθνικής ή εθνοτικής καταγωγής γενεαλογικών καταβολών, θρησκείας, αναπηρίας, σεξουαλικού προσανατολισμού, ταυτότητας ή χαρακτηριστικών φύλου το πλαίσιο ποινής διαμορφώνεται ως εξής: α) Στην περίπτωση πλημμελήματος, που τιμωρείται με φυλάκιση έως ένα (1) έτος, το κατώτερο όριο της ποινής αυξάνεται στους έξι (6) μήνες και το ανώτερο όριο αυτής στα δύο (2) έτη. Στις λοιπές περιπτώσεις πλημμελημάτων το κατώτερο όριο ποινής αυξάνεται κατά ένα (1) έτος. β) Στην περίπτωση κακουργήματος, που το προβλεπόμενο πλαίσιο ποινής ορίζεται σε πέντε (5) έως δέκα (10) έτη, το κατώτερο όριο ποινής αυξάνεται κατά δύο (2) έτη. Στις λοιπές περιπτώσεις κακουργημάτων το κατώτερο όριο ποινής αυξάνεται κατά τρία (3) έτη.	Article 21 of the law 4356/2015 Article 81A Crime with racist characteristics If the circumstances show that a crime has been committed against a victim, the choice of which was made by reason of the characteristics of race, colour, national or ethnic origin of genealogical payments, religion, disability, sexual orientation, identity or characteristics of sex, the penalty framework shall be as follows: (a) In the case of a misdemeanour punishable by imprisonment of up to one (1) year, the minimum sentence shall be increased to six (6) months and the maximum limit thereof to two (2) years. In other cases of misdemeanours the lower penalty limit shall be increased by one (1) year. (b) In the case of a felony, the prescribed penalty framework is set at five (5) to ten (10) years, the lower penalty limit is increased by two (2) years. In other cases of felonies the lower penalty limit is increased by three (3) years.
Αρ. 82α του ν. 4619/2019 Έγκλημα με ρατσιστικά χαρακτηριστικά Εάν έχει τελεστεί έγκλημα κατά παθόντος, η επιλογή του οποίου έγινε λόγω των χαρακτηριστικών φυλής, χρώματος, εθνικής ή εθνοτικής καταγωγής, γενεαλογικών καταβολών, θρησκείας, αναπηρίας, γενετήσιου προσανατολισμού, ταυτότητας ή χαρακτηριστικών φύλου, το πλαίσιο ποινής διαμορφώνεται ως εξής:	Article 82a of the law 4619/2019 Crime with racist characteristics If a crime has been committed against a victim, the choice of which was made because of the characteristics of race, colour, national or ethnic origin, genealogical payments, religion, disability, sexual orientation, identity or characteristics of sex, the penalty framework shall be as follows:

α) Στην περίπτωση πλημμελήματος, που τιμωρείται με φυλάκιση έως ένα έτος, το ελάχιστο όριο της ποινής αυξάνεται κατά έξι μήνες. Στις λοιπές περιπτώσεις πλημμελημάτων, το ελάχιστο όριο αυτής αυξάνεται κατά ένα έτος.	(a) In the case of a misdemeanour punishable by up to one year in prison, the minimum penalty shall be increased by six months. In other cases of misdemeanours, the minimum threshold shall be increased by one year.
β) Στην περίπτωση κακουργήματος το ελάχιστο όριο ποινής αυξάνεται κατά δύο έτη.	(b) In the case of a felony, the minimum penalty limit shall be increased by two years.
Αρ. 28 του ν. 4624/2019	Art. 28 of the Law 4624/2019
1. Στον βαθμό που είναι αναγκαίο να συμβιβαστεί το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς και για σκοπούς ακαδημαϊκής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται όταν: α) το υποκείμενο των δεδομένων έχει παράσχει τη ρητή συγκατάθεσή του, β) αφορά δεδομένα προσωπικού χαρακτήρα που έχουν προδήλως δημοσιοποιηθεί από το ίδιο το υποκείμενο, γ) υπερέχει το δικαίωμα στην ελευθερία της έκφρασης και το δικαίωμα της πληροφόρησης έναντι του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα του υποκειμένου, ιδίως για θέματα γενικότερου ενδιαφέροντος ή όταν αφορά δεδομένα προσωπικού χαρακτήρα δημοσίων προσώπων και δ) όταν περιορίζεται στο αναγκαίο μέτρο για την εξασφάλιση της ελευθερίας της έκφρασης και του δικαιώματος ενημέρωσης, ιδίως όταν αφορά ειδικών κατηγοριών δεδομένα Προσωπικού Χαρακτήρα, καθώς και ποινικές διώξεις, καταδίκες και τα σχετικά με αυτές μέτρα ασφαλείας, λαμβάνοντας υπόψη το δικαίωμα του υποκειμένου στην ιδιωτική και οικογενειακή του ζωή.	1. To the extent necessary to reconcile the right to the protection of personal data with the right to Freedom of Expression and information, including processing for journalistic purposes and for the purposes of academic, artistic or literary expression, the processing of personal data shall be permitted where: (a) the data subject has given his express consent; (b) relates to personal data which have been manifestly made public by the subject himself; (c) the right to Freedom of Expression and the right to information is prominent over the right to the protection of the personal data of the subject, in particular in matters of general interest or where it concerns personal data of public persons; and (d) where it is limited to the measure necessary to ensure Freedom of Expression and the right to information, in particular where it concerns specific categories of personal data, as well as criminal prosecutions, convictions and security measures relating thereto, taking into account the right of the subject to his private and family life.
Αρ. 11 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης Ελευθερία της έκφρασης και της πληροφόρησης	Article 11 of the Charter of Fundamental rights of the European Union 2012/C 326/02 Freedom of Expression and information 1. Everyone has the right to Freedom of Expression. This right shall include freedom

1. Κάθε πρόσωπο έχει δικαίωμα στην ελευθερία της έκφρασης. Το δικαίωμα αυτό περιλαμβάνει την ελευθερία να διαράττεται απόψεις και να λαμβάνεται και να μεταδίδει πληροφορίες και ιδέες χωρίς παρέμβαση της δημόσιας αρχής και ανεξαρτήτως συνόρων. 2. Γίνεται σεβαστή η ελευθερία και η πολυφωνία των μέσων ενημέρωσης.	to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.

Bibliography

English titles

Legislation

Universal Declaration of Human Rights

International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966

Convention for the Protection of Human Rights and Fundamental Freedoms (known as European Convention on Human Rights; ECHR)

The Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948, UN Treaty Series, vol. 78.

The Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998.

International Convention on the Elimination of All Forms of Racial Discrimination, 21 December 1965, UN Treaty Series, vol. 660

ICERD Committee, CERD/C/GC/35, 9 September 2013.

Convention on Cybercrime (ETS no. 185).

Treaty on the Functioning of the European Union (TFEU)

Charter of Fundamental Rights of the European Union

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

Regulation 679/2016 (EU) of the European Council and of Council of 27 April 2016 on the protection of natural persons against the processing of their personal data and the free movement of such data; and repealing the Directive 95/46/EC (General Regulation on Data protection)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004)

Directive (EU) 2016/680 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) L 108/33

Recommendation No.R(97)20 of the Council of Europe Committee of Ministers on 'Hate Speech,' 30 October 1997

Reports

Opinion WP 225, 26.11.2014, Working Party of Article 29, Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12, https://ec.europa.eu/justice/Article-29/documentation/opinion recommendation/files/2014/wp225_en.pdf

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) in his annual report to the General Assembly, A/76/357, 7 September 2012

Internet: case law of the European Court of Human Rights, June 2015, by the Council of Europe.

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/17/27, La Rue F. (16 May 2011).

Books

Claire Wardle, Hossein Derakhshan, Information Disorder; Toward an interdisciplinary framework for research and policymaking, by theCouncil of Europe

'Hate Speech' Explained, A Toolkit, (2015), by the Council of Europe

Wolfgang Benedek and Matthias C. Kettemann, 'Freedom of Expression and the Internet', (2013), by the Council of Europe

Pitsela T., Chatzispyrou A., (2017),'Criminal policy developments against racism in Greece', Ant. N. Sakkoulas Publications L.P. 2017

Periodicals

Banks J., 'Regulating Hate Speech Online', (2010), International Review of Law, Computers & Technology Vol. 24, No.3 , 233- 239.

Christopher D. Van Blarcum, 'Internet Hate Speech: The European Framework and the Emerging American Haven', (2005).

Tsakyrakis S., 'Proportionality: An assault on human rights?', International Journal of Constitutional Law, Vol.7, Issue 3, (July 2009).

Digital resources

https://eur-lex.europa.eu/.

https://www.echr.coe.int/.

https://www.ohchr.org/.

https://www.un.org/.

Owen Bowcott, *'Facebook to be subject to tougher controls after EU court ruling; ECJ says member states can order platform to remove defamatory material globally',* The Guardian, available online at;https://www.theguardian.com/technology/2019/oct/03/facebook-faces-tougher-controls-after-eu-ruling.

OSCE Permanent Council Decision No. 633 (PC.DEC/633 of 11 November 2004), *'Decision no. 633 promoting tolerance and media freedom on the Internet'*, 532nd Plenary Meeting PC Journal No. 532, Agenda item 5, available online at;

https://www.osce.org/pc/16912?download=true,

https://www.whoishostingthis.com/blog/2017/02/27/internet-censorship/.

https://globalfreedomofexpression.columbia.edu/cases/.

Protalinski E. (15 November 2011), 'Facebook name battle: Ahmed Salman Rushdie claims victory',

www.zdnet.com/blog/facebook/facebook-name-battle-ahmed-salman-rushdie-claims-victory/5358.

G. Stavropoulos, 'The influence of ECHR on the Greek law order' ,https://www.constitutionalism.gr/stavropoulos-esda-elliniki-ennomi-taxi/.

Thesis of Papas I, 'The protection of personality in the net', (2011), https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1322688/theFile/1322689.

Case law

CJEU, judgment of 18 October 2018, *Bastei Lübbe GmbH & Co. KG v Michael Strotzer*, Case C-149/17, ECLI:EU:C:2018:841

CJEU, Judgment of 16 July 2015, *Coty Germany*, C-580/13, EU:C:2015:485

CJEU, Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317

ECHR, Gündüz v. Turkey, no. 35071/97

ECHR, Kącki v. Poland, no. 10947/11

ECHR, K.U. v. FinLand, no. 2872/02.

Greek titles

Legislation

Το Σύνταγμα της Ελλάδος

Αστικός Κώδικας

Ποινικός Κώδικας

Κώδικας Πολιτικής Δικονομίας

Νόμος 4619/2019 - ΦΕΚ 95/Α/11-6-2019 - Κύρωση του Ποινικού Κώδικα

Νόμος 4624/2019 - ΦΕΚ 137/Α/29-8-2019 - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων & Αιτιολογική Έκθεση

Νόμος 4356/2015 - ΦΕΚ 181/Α/24-12-2015 - Σύμφωνο συμβίωσης, άσκηση δικαιωμάτων, ποινικές και άλλες διατάξεις

Νόμος 4285/2014 - ΦΕΚ 191/Α/10.9.2014 - Τροποποίηση του ν. 927/1979 (Α' 139) και προσαρμογή του στην απόφαση πλαίσιο 2008/913/ΔΕΥ της 28ης Νοεμβρίου 2008, για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου (L 328) και άλλες διατάξεις.

Νόμος 4267/2014 - ΦΕΚ Α 137/12-6-2014 - Καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις.

Νόμος 4072/2012 - ΦΕΚ Α'86/11-4-2012 -Βελτίωση επιχειρηματικού περιβάλλοντος - Νέα εταιρική μορφή - Σήματα - Μεσίτες Ακινήτων - Ρύθμιση θεμάτων ναυτιλίας, λιμένων και αλιείας και άλλες διατάξεις.

Νόμος 4070/2012 - ΦΕΚ Α' 82/10-04-2012 - Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις

Νόμος 3603/2007 - ΦΕΚ 188/Α/8-8-2007 - Ρύθμιση θεμάτων δημοσκοπήσεων

Νόμος 3471/2006 - ΦΕΚ 133/Α'/28-6-2006 - Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997

Νόμος 2472/1997 - ΦΕΚ Α'50 /10-4-1997 - Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Νόμος 2121/1993 - ΦΕΚ Α'25/3-3-1993 - Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα

Νόμος 1178/1981 - ΦΕΚ 187/Α/16-7-1981 - Περί αστικής ευθύνης του τύπου και άλλων τινών διατάξεων

Προεδρικό Διάταγμα 131/2003 - ΦΕΚ Α' 116/16-05-2003 - Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο).

Books

Γιαννόπουλος Γιώργος, «Οι ευθύνες των παρόχων υπηρεσιών online»

Δαγτόγλου, «Συνταγματικό δίκαιο, ατομικά δικαιώματα»

Καρακώστας Ιωάννης, (2009), «Νόμος και Διαδίκτυο» , Π.Ν. Σάκκουλας

Κοτσάλης και Μενουδάκος, (2018), «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR) Νομική διάσταση και πρακτική εφαρμογή», Νομική Βιβλιοθήκη

Γεωργιάδης, (2012) «Γενικές Αρχές Αστικού Δικαίου», 4η έκδοση, Εκδόσεις Σάκκουλας

Χρυσόγονος, (2006), «Ατομικά και Κοινωνικά Δικαιώματα», 3η έκδοση, Νομική Βιβλιοθήκη

Παντελής Α., (2016), «Εγχειρίδιο Συνταγματικού Δικαίου», Εκδόσεις Λιβάνη

Βλαχόπουλος Σ., (2017), «Θεμελιώδη Δικαιώματα» , Νομική Βιβλιοθήκη

Periodicals

Media and Communications Law

Δίκαιο και ΜΜΕ

Απόστολος Τασίκας, Άρση από Τρίτο της Προσβολής Προσωπικότητας (σε Ευθύνη από Προσβλητικό Περιεχόμενο Αναρτήσεων στο Διαδίκτυο) (2019) τεύχος 3, Δίκαιο και ΜΜΕ

Δ.Μ. Παπαδοπούλου, ΕΔΔΑ απόφ. της 19.2.2013, υπόθ. Neij and SundeKolmisoppi v. Sweden προσφ.No 40397/2012 [Ανταλλαγή αρχείων στο Διαδίκτυο] (2013) τεύχος 1, Δίκαιο και ΜΜΕ

ΣτΕ 2112/1984, Το Σύνταγμα (1985) 63

Γ. Γιαννόπουλος, ΕΔΔΑ απόφ. της 4.12.2018 υπόθ. MagyarJ etiZrt κατά Ουγγαρίας προσφ.No 11257/16 (Τέταρτο Τμήμα) [Ευθύνη από χρήση υπερσυνδέσμου] (2019) τεύχος 1, Δίκαιο και ΜΜΕ

Ε. Τσεκούρα, Διακοπή πρόσβασης σε παράνομο περιεχόμενο στο Διαδίκτυο: Η λειτουργία της ΕΔΠΠΙ και οι προκλήσεις για το μέλλον (2018) τεύχος 4, Δίκαιο και ΜΜΕ

Γ. Γιαννόπουλος, Ειδοποίηση και Απόσυρση (Notice&Take-Down): Η επανεμφάνιση της διαδικασίας και η εφαρμογή της (2016) τεύχος 1, Δίκαιο και ΜΜΕ

Digital resources

Greece Study on blocking, filtering and take-down of illegal Internet content

Case law

Απόφαση υπ' αριθμ. 25/2019 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 41/2017 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 82/2016 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων.

Απόφαση υπ' αριθμ. 83/2016 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 84/2016 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 17/2016 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 13/2011 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Γνωμοδότηση υπ' αριθμ. 4/2011 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 17/2008 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 2/2006 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 23/2005 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Γνωμοδότηση υπ' αριθμ. 1/2001 της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων

Απόφαση υπ' αριθμ. 1/2018 της Επιτροπής για την Γνωστοποίηση Διαδικτυακής Προσβολής Δικαιωμάτων Πνευματικής Ιδιοκτησίας και Συγγενικών Δικαιωμάτων

Απόφαση υπ' αριθμ. 174/2017 του Πρωτοδικείου Βόλου

Απόφαση υπ' αριθμ. 1143/2016 του Εφετείου Αθηνών

Απόφαση υπ' αριθμ. 3799/2015 του Πολυμελούς Πρωτοδικείου Αθηνών

Απόφαση υπ' αριθμ. 13478/2014 του Μονομελούς Πρωτοδικείου Αθηνών

Απόφαση υπ' αριθμ. 5635/14 του Πρωτοδικείου Αθηνών

Απόφαση υπ' αριθμ. 4658/2012 του Πρωτοδικείου Αθηνών

Απόφαση υπ' αριθμ. 22228/2011 του Πρωτοδικείου Θεσσαλονίκης

Απόφαση υπ' αριθμ. 164/2011 του Εφετείου Αθηνών

Απόφαση υπ' αριθμ. 25552/2010 του Πρωτοδικείου Θεσσαλονίκης

Απόφαση υπ' αριθμ. 4042/2010 του Πρωτοδικείου Αθηνών

Απόφαση υπ' αριθμ. 965/2010 του Τριμελούς Πλημμελειοδικείου Κιλκίς

Απόφαση υπ' αριθμ. 4980/2009 του Πρωτοδικείου Πειραιά

Απόφαση υπ' αριθμ. 543/2009 του Αρείου Πάγου

Απόφαση υπ' αριθμ. 44/2008 του Μονομελούς Πρωτοδικείου Ροδόπης

Απόφαση υπ' αριθμ. 195/2007 του Αρείου Πάγου

Απόφαση υπ' αριθμ. 8661/2000 του Εφετείου Αθηνών

Απόφαση υπ' αριθμ. 9099/2005 του Εφετείου Αθηνών

Απόφαση υπ' αριθμ. 65/2004 του Πολυμελούς Πρωτοδικείου Αθηνών

Απόφαση υπ' αριθμ. 8661/2000 του Εφετείου Αθηνών

Απόφαση υπ' αριθμ. 5783/1997 του Εφετείου Αθηνών

ELSA Hungary

Contributors

National Coordinator

Bálint Imre Bodó

National Academic Coordinator

Dr. Kitti Dalma Kürthy

National Researchers

Annamária Durucskó

Bálint Imre Bodó

Dávid Szkladán

Dr. Kitti Dalma Kürthy

Zsófia Márta Tengölics

National Linguistic Editor

Dr. Márta Tengölics

Acknowledgements

Special thanks to family, and friends, who always supported us, during this journey.

Introduction

Hungary is one of the EU-27 States, that must comply with the international standards just as much with his own Constitution. It surely is not surprising, that the question raised usually goes hand in hand with constitutional law.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

People are largely free to participate in politics without encountering undue influence over their political choices.

Women are underrepresented in political life, holding no cabinet posts and only 20 out of 199, seats in the National Assembly. This 10 percent ratio represents the lowest percentage in the EU, with even lower representation, 7 percent, among ruling party lawmakers.

Hungary's constitution guarantees the right of ethnic minorities to form self-governing bodies, and all 13 recognised minorities have done so. Minorities can also register to vote for special minority lists – with a preferential vote threshold – in parliamentary elections, but they are then excluded from general party-list voting. None of the 13 minority lists won enough votes to secure a seat in 2014, meaning each is represented only by a nonvoting spokesperson.

The constitution guarantees religious freedom and provides for the separation of church and state, although these guarantees were weakened in the 2011 constitution, whose preamble now makes direct references to Christianity, including the recognition of 'the role of Christianity in preserving nationhood.' Nevertheless, adherents of all religions are generally free to worship their Gods.

A gradual overhaul of the public education system has raised concerns about excessive government influence on school curriculums: legislation adopted in 2014 allows for government-appointed chancellors to make financial decisions at public universities.

In April 2017, lawmakers adopted amendments to the higher education law that targeted Central European University (CEU), a postgraduate institution with dual American-Hungarian accreditation founded by the Hungarian-born international financier and philanthropist George Soros.

The amendments, which codified burdensome new requirements that effectively made CEU unlawful, was widely denounced, including by the Council of Europe's Venice Commission, which recommended their repeal, and by the European Commission, which opened an infringement procedure over the issue. In October, the government extended the deadline for compliance with the amendments by one year, and it could be said that the CEU was successfully complied with.

While freedom of expression is constitutionally protected, but media has left a chilling effect on private speech, particularly online speech. The threat of defamation suits or other retribution for criticism of authorities also contributes to this environment, though courts mostly refuse to apply sanctions for what they see as protected speech.

Echo chambers – the lack of different opinions on a certain issue – are threatening people's right to information in the modern age. In today's world of a social media saturated with fake and sensational news, and an online media fighting for page views, the echo chamber effect is growing, and those media outlets that pride themselves on professional journalism have a special obligation to promote discourse.

Since the 19th century, creating a Commission in the event of child pornography, state crime or acts of terrorism (in other cases as a given possibility) became mandatory.

The NAV (National Tax Office) is obliged to block the websites of prohibited gambling operators.

From 2015 onwards, drug trafficking, pathological addiction, promotion of drug production, drug precursor abuse, abuse of new psychoactive substances and financing of terrorism criminal have also been placed among mandatory cases of inaccessibility.

In addition, from this year, NAV can block websites organising illicit gambling.

From 2016, the National Transport Authority (NCA) may block the 2012 Directive on passenger transport services. In the 2004 act, the Commission the website of service providers for which it has imposed fines for the absence of a

licence and the fined service provider continued to operate without authorisation.

It is clear that there is no longer any question regarding the court's involvement in blocking content. The fully autonomous decision of the NCA and NAV is perfectly sufficient to start blocking content. Any notices, descriptions or even a factsheet on the NKH's website, which indicated blocking, could not be found.

However, it was necessary to expand the system not only legally, but also technically. Perhaps many people would not think that KEHTA set the foundations for just over 7 million forints on behalf of NMHH by Interface Computing Ltd.

Hungary's laws ensure that people have the opportunity to access data of public interest (or data declared to be of public interest by law) if the data controller is performing a public function, the information is related to their activities and the data is under their control.

If the court agrees with an individual's petition, it will make the data controller share the requested data of public interest with them. The court is entitled to modify the sum of the fee charged for making a copy or order the launch of a new procedure to determine an appropriate fee.

Public organs and institutions, especially those involved with budgetary, financial, or contractual matters, must not only allow access to data of public interest upon request, but they must also ensure that accurate and expedient information is readily available.

The data controller is obliged to make up-to-date data of public interest plainly available on either their own websites or on a centralised website. They may not make access dependent on the disclosure of personal identification information. Detailed information about how to submit a request for public data must be clearly provided on the website and the website must also include information about options for legal redress.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

Internet access is widespread in Hungary. Internet prices remain relatively high compared to Hungary's European neighbours, and a rural-urban divide in access persists. The internet and mobile markets remain concentrated among a handful of providers.

Levels of access differ based on geographical and socio-economic conditions, with lower access rates found among low-income families and in rural areas. Internet penetration also differs between those living in the capital and in the countryside. A digital divide based on ethnicity has also been observed, with the Roma community historically having lower levels of internet access.

The government does not restrict bandwidth, routers, or switches, and backbone connections are owned by telecommunications companies rather than the state.

Legally, however, the internet and other telecommunications services can be paused or limited in instances of unexpected attacks, for pre-emptive defence, or in states of emergency or national crisis.

Having said this, it is observed that the ICT market in Hungary lacks significant competition, with over a third of the market belonging to Magyar Telekom. Four ISPs control over 80 percent of the total fixed broadband market.

There are three mobile phone service providers, all privately owned by foreign companies. Mobile internet network expansion has been relatively stagnant because of the lack of competition. A fourth provider, Romanian-owned Digi acquired frequencies to offer services in 2014 and was expected to launch in June 2018.

2.1. Regulatory Bodies

The National Media and Infocommunications Authority of Hungary (NMHH) and the Media Council, established under media laws passed in 2010, are responsible for overseeing and regulating the mass communications industry. The Media Council is the NMHH's decision-making body in matters related to media outlets, and its responsibilities include allocating television and radio frequencies and penalising violators of media regulations. The Head of the Media Council appoints the president of the MTVA, the fund responsible for producing content for the public service media. The members of the Media Council are nominated and elected by parliamentary majority, then appointed by the President of the Republic. The Head of the NMHH is appointed by the president based on the proposal of the prime minister, for a non-renewable nine-year term.

With the adoption of the Fundamental Law of Hungary, which entered into force in January 2012, the governing parties prematurely ended the six-year term of the Data Protection and Freedom of Information Commissioner, replacing the former office with the National Authority for Data Protection and Freedom of Information. The head of the new authority is appointed by the president of

the republic based on the proposal of the prime minister for a nine-year term and can be dismissed by the president based on the proposal of the prime minister, calling into question the independence of the agency.

In 2014, the Court of Justice of the European Union ruled that Hungary failed to fulfil its obligations under EU law when it ended the Data Protection Commissioner's term.

2.2. Limits on Content

The government of Hungary does not engage in any significant blocking of content online and does not place restrictions on access to social media, though a number of websites purportedly containing Holocaust denial content were blocked by the authorities.

Online content is somewhat limited as a result of lack of revenue for independent media outlets online, the dominance of the state-run media outlet, and the biased nature of the allocation of state advertisement funds.

The authorities often block content under Hungarian laws banning public Holocaust denial. In August 2016, a Hungarian court ordered the blocking of 20 websites that contained material denying the Holocaust.

In January 2015, the Metropolitan Court of Justice ordered the far-right website Kuruc.info to delete an article denying the Holocaust.

2.3. Blocking and Filtering

The government does not place any restrictions on access to social media or communication applications. YouTube, Facebook, Twitter, international blog-hosting services, instant messaging, and other applications are freely available.

The penal code, in effect since 2013, includes provisions based on which websites can now be blocked for hosting unlawful content. The law stipulates that if the illegal content is hosted on a server located outside of the country, the Hungarian court will issue a query to the Minister of Justice to make the content inaccessible; the minister then passes the query onto the 'foreign state,' and if there is no response from that state for 30 days, the court can order domestic ISPs to block the content.

The prosecutor, ISP, and the content provider can appeal the court order within eight days of the decision. The NMHH is the authority designated to manage the list of websites to be blocked based on court orders. The list, referred to as KEHTA (Hungarian acronym for 'central electronic database of decrees on

inaccessibility'), went into effect on 1 January 2014 with the primary aim of fighting child pornography.

2.4. Content Removal

Though the law in Hungary generally protects against intermediary liability for content posted by third parties, in some cases courts have held individuals responsible for third-party comments on their websites.

As an example, in early 2016, László Toroczkai, far-right politician and mayor of Ásotthalom, was held liable by a court for 'disseminating' defamatory comments posted by another person on his Facebook page. The court found that, by allowing commenting on his page, Torockai had accepted responsibility for any unlawful content posted by others. The comments said a journalist 'should be hanged.'

Another case occurred in June 2015, when the popular news website 444.hu was held liable for publishing a hyperlink to a YouTube video which undermined the reputation of Jobbik, a far-right party. The court found that by publishing the hyperlink, 444.hu had assumed liability for the defamatory content contained in the YouTube video. The case is expected to be decided by the European Court of Human Rights (ECtHR) in 2018.

The Court found that the Hungarian domestic law on objective (strict) liability for disseminating defamatory material had excluded the possibility of any meaningful assessment of the applicant

company's Right to Freedom of Expression in a situation where the courts should have scrutinised the issue carefully.

Such objective liability for using a hyperlink could undermine the flow of information on the Internet, dissuading article authors and publishers from using such links if they could not control the

information they led to. That could have a chilling effect on freedom of expression on the Internet. Overall, the applicant company had suffered an undue restriction of its rights.

In an earlier case decided in February 2016, ECtHR ruled that Hungarian courts had failed to properly balance the right to reputation and the right to freedom of the press by holding websites liable for comments posted on their pages.

According to Hungarian legislation, intermediaries are not otherwise legally responsible for content if they did not initiate or select the receiver of the transmission, or select or modify the transmitted information.

Intermediaries are also not obliged to verify the content they transmit, store, or make available, nor do they need to search for unlawful activity. Hosting providers are required to make data inaccessible, either temporarily or permanently, once they receive a court order stating that the hosted content is illegal.

However, both print and online media outlets bear editorial responsibility if their aim is to distribute content to the public for 'information, entertainment or training purposes.'

The law fails to clarify what editorial responsibility entails and whether it would imply legal liability for online publications. A member of the Media Council said that the provision could apply to a blog if it generates revenue and is registered as a media content provider by the NMHH.

Further, the law states that constitutional order and human rights must be respected, and that public morals cannot be violated.

However, the law does not define the meaning of 'any majority' or 'public morals.' If a media outlet does not comply with the law, the Media Council may oblige it to 'discontinue its unlawful conduct,' publish a notice of the resolution on its front page, and/or pay a fine of up to HUF 25 million (approximately US$93,000). If a site repeatedly violates the stipulations of the media regulation, ISPs can be obliged to suspend the site's given domain, and as a last resort, the media authority can delete the site from the administrative registry.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

An internet content may be blocked or removed on civil law criminal law or on administrative law bases, but under different procedures.

3.1. Right to integrity and reputation

First of all, the Fundamental Rights of Hungary (hereinafter the Constitution), declares that everyone shall have the Right to Respect for his or her private and family life, home, communications and reputation. Therefore, it also declares, that exercising the right shall not result in violating the private and family life, and the home of others.

The protection of these Rights is manifested in the Rights contained in the personality section of the Hungarian Civil Code (hereinafter: Civil Code). The

Civil Code entitles the person whose personality rights have been violated to demand the termination of the injurious situation and the restoration of the previous state. If the violation of a personal right occurs in an internet content the entitled person can demand from the violator to remove that content. Under the Civil Code the personal rights of the injured person may be enforced by way of judicial process.

From the point of view of internet content, the Right to Integrity and the Right to Reputation are particularly important among other personality rights. For instance, the protection of the Right to Integrity restricts the protection the Freedom of Expression. The Civil Code ensures the balance between these Rights by declaring that everyone is entitled to freely practice their personality rights but just within the rights of others.

When the infringing content is published by an online (or any other) journal, the law provides additional protection against violation of the right to reputation. The extent of publicity necessarily agonises the consequences of the infringing content, especially in the case of online journals. Therefore, where published media content disseminates false facts or distorts true facts about a person, the person affected shall be entitled to demand the publication of an announcement to clearly identify the false, distorted and/or unfounded facts of the communication and indicate the true facts. The remedy communication shall be published in the case of online journals within five days upon receipt of the request thereof, using the means similar in style and size as the contested part of the communication.

The only function of the Right to remedy is to correct the allegedly false content, within a short period of time, if the violator cannot prove immediately that the content is true. It gives the entitled person an opportunity to present a compensatory statement against a statement containing facts that are not immediately verifiable. The publication of a statement retraction may be demanded by the affected person within a preclusive period of thirty days from the date of publication of the disputed communication. If the press organisation fails to comply with such obligation in due time the person requesting the retraction may enforce its right through civil procedural means before the civil court.

Under the Hungarian law, the extent of the restriction of Freedom of Expression is different in cases where the injured person is a politically exposed person. In this case person's rights are diminished in order to ensure the enforcement of the exercise of fundamental rights relating to the free debate of public affairs

considering the criteria of necessity and proportionality, without causing any harm to human dignity.

3.2. Blocking and removing of internet content on criminal base.

The Right to Integrity and the Right to Reputation are also protected by the Hungarian Criminal Code by prohibition of defamation and slander, but under different and stricter conditions. The Criminal Law in this regard thus also restricts the Right to Freedom of Expression but under a narrower scope. Furthermore, the Criminal Code protects the human dignity and private life by prohibiting, inter alia, 'desecration' which occurs if defamation or slander violate a dead person, 'mail fraud' and 'invasion of privacy' which crimes are protecting the private secret or 'misuse of personal data'. These offences often regard a published internet content. The Criminal Code ensures, appropriate protection against these crimes by declaring the opportunity to irreversibly rendering electronic information inaccessible as a measure against the committed crime.

This measure is ordered independently or in addition to the penalty, thus this measure shall be issued even if the perpetrator cannot be prosecuted for reason of minority or insanity or due to other grounds for exemption from criminal responsibility. Every data disclosed through an electronic communications network shall be rendered irreversibly inaccessible. Therefore, the judge through the judgement shall order the removal of any content on internet which contains any of these data.

3.3. Child protection

In addition to the reasons declared by Civil Law and Criminal Law there are other reasons that may cause the blockage or the removal of an internet content. In this regard the most important reason is child protection. The protection of the child is ensured concerning media content and other online service provider's content. Related to the media content the Act CIV of 2010 on Freedom of the Press and on the Basic Rules Relating to Media Content declare that any media content featured in media services which is likely to impair the mental, spiritual, moral or physical development of minors may be made available to general audiences only if it is ensured − in particular by selecting the time of the broadcast, by using age verification tools or by any technical measure − that minors in the area of transmission will not normally hear or see such broadcasts. Access control measures shall be proportionate to the potentially harmful nature of the content. Furthermore, any media content featured in a press product which might seriously impair the physical, mental or moral development of minors, in particular those that involve pornography or extreme

or explicit scenes of violence, may be published and made available to general audiences only in such a way as to ensure - by means of technical or other similar safeguards – that minors will not be able to access them. If such safeguards are not available, the media content in question may be published only with a warning concerning the potential endangerment to minors. Media contents may not feature minors in a way that is likely to seriously impair the minor's mental or physical development taking in account their age.

Furthermore, the Hungarian law provides for the minor or their legal representative, whose personality rights are alleged to have been infringed upon by any information to which a service provider has given access too, to demand the deletion of the content. The service provider may refuse to block access to the information contested if it considers the accusation of infringement unfounded. If the service provider refuses the claim, the minor or his legal representative can claim the blocking from the Round-table Conference. The round-table Conference has the right to investigate reports on a case by case basis, and to publish non-binding recommendations or opinions relying on the general conclusions thereof. Such procedure may only prevent the intervention of the competent court but not exclude it.

3.4. Protection of IP rights

The interest of an intellectual property right holder (inter alia: copyright, trademark or geographical indication) can also constitute the legal ground for the internet content blocking. Any proprietor, whose executive rights relating to any intellectual property are alleged to have been infringed by an internet content, is entitled to notify the service provider for removing the information in question. Thus, the right holders also have an additional right beside the civil legal procedure similar to the minor. The service provider shall take the measures necessary for the removal of the information in question and shall inform the proprietor that the information was taken down within twelve hours following the receipt of the notification. Otherwise it can take an objection against the removal of the information contested. This procedure neither exclude nor substitutes the legal procedure of the competent court. The purpose of this provision is to enable the right holder to block or remove access to information that is allegedly infringing his rights, before initiating a litigation that is often lengthy, for the purpose of establishing an infringement and pursuing further claims.

3.5. Combat against illegal gambling

The Gaming supervisory authority shall order the rending of information published by way of an electronic communications network inaccessible temporarily the publication or disclosure to constitute illegal gambling operators. It means the temporary blocking of the information, for a period of 365 days. The Gambling supervisory authority shall abolish the blocking before it is terminated if based on request made by the criminal court or the grounds therefor no longer exist. The NMHH shall organise and monitor the execution of rendering electronic information temporarily inaccessible.

The service provider where the blocking was ordered by an authority can, in any case claim remedy from the competent Hungarian court in accordance with the Hungarian administration litigation rules.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In Hungary, there is an association namely The Association of Hungarian Content Providers (MTE) which is a self-regulating body. It was founded in 2001 by a Hungarian internet content providers order for the content providers to be able to participate in the development of the Hungarian Internet business market with verified and professionally supported commitments, and with the tools of self-regulation.

One of the main focuses of MTE to achieve that the Internet be regulated with the smallest state intervention possible, and that emphasis is placed on self-regulation. For this, MTE created the professional code of internet content providing, and the code of ethics describing a generally accepted system of ethical norms for Hungarian content provision.

The Code of the association is binding only for their members.

Under the association's Code, Internet Content Provider shall be every legal or natural entity, or any groups thereof, publishing any type of (textual, numerical, visual, audio, or multimedia) information, restricted or unrestricted in time, and accessible by the collectively, or any group, of Internet users in a way that this legal or natural entity can be definitely identified by those accessing such content.

The Ad Hoc Committee of experts of the Hungarian Association of Content Providers is in charge of applying the rules.

The Committee starts procedures only at request. At request, the Committee takes a stand on concrete, individual cases regarding the interpretation of the Code, as well as in all situations where the object of procedure does not concern the violation of the Code but involves taking a stand in a dispute between the concerned parties.

Any person is entitled to submit a claim to the Committee if the conduct that is contrary to the rules of the Code interferes with his rights or rightful interests or, otherwise if he is a member of the Association or he is interested in the statement of the Committee to be made as a result of its procedure.

In case of non-compliance with the rules, the claim should be submitted within 15 days from the supervening of the infringement or when the infringement is recognised by the claimant only later, the 15 days deadline starts with the recognition of the infringement, or the disappearance of the impediment.

Upon receiving the claim, the Committee in delivering the complete claim, invites the appealed person to reach an agreement with the appellant within five days and to submit it with the appellant for approval by the Commission. If they cannot agree, it advises the appealed party to submit its written notes and incidental counterclaim, attaching the supporting evidence, to the Committee within three days. Therefore, in the proceeding of the Association the right to be notified of a takedown request and to object to the same model applied. In the resolution by the Committee closing the proceedings substantiated claims are approved and the infringement of norms is established by indicating the relevant provisions of the Code, when necessary, the appealed is obligated to change its breaching conduct and restore the original state of affairs. Depending on the severity of the offense, the appealed may be banned from practicing its entitlements for a certain period, with respect to announcing its belonging to the Association and its use as a reference or other rights originating in membership, e.g. the right to vote, enjoyed by the claimant, may be suspended for a certain period of time or the appealed may be excluded from membership in the Association in case of repeated offense of rules. The decision regarding the affair is always published on the homepage of the Association.

The procedure code of the Association prove remedy against the decisions of the AD HOC committee by in case of the infringement of procedural rules, the parties may appeal against the resolution of the Committee. Appeals, addressed to the President of the Association, must be submitted within eight days at the Secretariat of the Association. In cases of disciplinary offense, the general assembly is authorised to make a second-degree resolution.

Any person is entitled to submit an indication to the Association if he perceives a content published by a member of the association contains offensive or false information or otherwise ethically problematic in accordance with the Ethical Code of the Association. The most popular online media service provider are members of the Association as the Index.hu Zrt.; Origo Zrt.; Napi.hu Online Kft. or the Centrál Médiacsoport Zrt.

The Code of the Association ensures appropriate procedures in order to prove ethical online governing without state intervention. Notwithstanding the decisions of the Committee or the Secretariat of the Association just bind on the members and has soft binding effects as the ultimate sanction is the exclusion from the members. Regarding the self-regulatory procedure, since there is no way to investigate violations of the law, the Hungarian Association of Content Providers is only entitled to take action in case of violation of its provisions. Against violation of any law, just the Hungarian competent court or the authority entitled to take action in accordance with the relevant procedure rules by the law.

Thus, the Association has no binding force in disputes between a rights holder or defamed person and a host.

Furthermore, every association is under legal control. Based on the public prosecutor's charges the competent civil court shall dissolve the association if it operates in violation of the law.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information - and several sectorial laws remained in force in unchanged form. The Act its interpretative provisions give the exact concept of cancellation. Data erasure means making data unrecognisable in such a way that it is no longer possible to recover it. Pursuant to Article 18 (1) of the Act, the deletion must be notified to the data subject and to those to whom the data have previously been transmitted for data management purposes. Notification may be dispensed with if this is not contrary to the legitimate interests of the data subject, having regard to the purpose of the processing.

6. How does your country regulate the liability of internet intermediaries?

In Hungary, the provisions of the E-Commerce Directive were adopted in accordance with the procedure for the application of the 2001 E-Commerce Directive. The commission shall, take it into law on e-commerce and the 2001 Act on E-Commerce. The commission shall, in the first place, take into the electronic signature.

From year 2011, the media law, which comes into force on 1 January 2014, allows in principle to control the Internet at a central level, since, unlike the previous law, it does not discriminate between traditional and new media platforms: all of them are. For content published on internet press outlets, websites and forums, the Internet Service Provider (ISP) is responsible as if it were providing an e-commerce-related service.

Therefore, if the ISP does not remove the damaged content at the request of the victim or the media supervisory authority, they shall act as if he were the content provider himself. At present, however, there is no judicial practice in deciding disputes arising from the media law.

The Supreme Court ruled that the trademark infringement was committed not only by a user who registered a domain name that was very reminiscent of an existing brand, but also the authority registering the domain name, which must have known the similarity of the name of the trademark. The Court, therefore, did not regard the service provider as merely an administrative function and thus found the responsibility of the service provider for his activities, since he had actively contributed to the offence by his orherion.[976]

The following is the responsibility of the host provider of the website that illegally uses (abused) imagination of minors. The Hungarian website pedomaci.hu dealt with the 're-use' of images uploaded to other storage sites – social media – by providing them with sexually charged addresses and comments, they posted on the website. However, the website's direct purpose was not to harm the offending (even if it ultimately achieved this with its defamatory or personal data) but to obtain revenue from advertisements placed on the website.

The website's host provider was a so-called anonymisation service provider, which promised anonymity to uploaders of the websites hosted by him. In 2009

[976] Spindler, G.: Study on the Liability of Internet Intermediaries. Country Report - Hungary, 2007 <http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_ en.pdf> accessed 21 February 2020.

and 2010, hotline and police received numerous reports from parents of children in the recordings, as the images were posted on the website without their consent and defamatory comments. The domain name of the website was removed by the registration authority at the behest of the hotline and civil rights organisations, saying that the name of the website itself is illegal, since it refers to the sexual exploitation of children. However, at the request of the hotline, the host provider removed the offensive content, but the website was then re-uploaded to another host pedomaci.net provider based in the US, so the website was similar content and purpose remain available.

Since, according to the prevailing interpretation of the law, the activities of the content provider itself do not constitute a criminal offence (due to the 'active public communication' of the victims), it remains unclear how the court would judge the host provider of the website and the responsibility of other users (editors) who place their ads on the website, who use the high-hits of the bot-page website to promote their ads. The liability of the intermediary (anonymisation) service provider may also arise, but since it is not obliged to monitor the activities of users of its services. The only official step taken in connection with the removal of the website was the involvement of the website's name registration authority. However, it can be stated, as indicated by the complaint letter submitted by the website operator to the domain registration authority, that the name of the website alone did not constitute the abusive content.

The technique, level and ideology of blocking must be carefully chosen so that fundamental rights remain intact, but blocking also serves its purpose. Internet filtering techniques are of particular concern because of their interference with fundamental rights: content owners 'freedom of opinion, users' access to information, and, depending on blocking techniques, telecommunication secrets may be compromised. Due to the nature of the Internet, almost all blocking methods can be bypassed and are not really effective.[977]

State-level blocking does not provide full protection and suffers from deficiencies and, partly because of these deficiencies, does not respect basic digital rights. However, it has also been seen that the self-regulatory solutions applied by service providers are not suitable in themselves for filtering out illegal content. The regulation of the Internet cannot be solved solely by self-regulation

[977] For a public discussion by the Committee on Civil Liberties on the introduction of an EU-wide internet blockade, see EDR-gram Number 9.1, 12 January 2011 <http://www.edri.org/book/export/html/2491>.

or by central control: a combination of actors in the two areas can provide the right solution.

This concentration is also necessary in the sense that the state's efforts to block the Internet cannot be realised without the active involvement of ISPs. But the reverse is also true: the self-regulatory mechanisms of ISPs can only work properly with the political or material support of the state or the market.

The EU clearly regulates the liability of the intermediary service provider. However, given the wide scope of the issue and the divergent case law created by states to interpret directives, the practice of applying the rules is far from clear.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1 Legislation regarding online content blocking and takedown in the next five years

On 11 February, on the day of the Safer Internet in Hungary, the National Media and Communications Authority (NMHH) published statistics from its Internet Hotline legal aid service last year, which showed that they were receiving more and more content depicting the sexual exploitation of children. [978]

The number of reports of material recording children's sexual exploitation has increased significantly, threefold compared to 2018. Nearly a third of notifications in this category were presumed to be child pornography. These cases were sent to the National Bureau of Investigation (NNI) for further action by hotline staff or, if the content was on a foreign server, through the inhope system of the umbrella organisation that brings together hotlines. The outstanding number of reported child pornographic content received in 2019, in addition to increasing domestic attention, can also be explained by the fact that the Canadian Centre of Child Protection project, Arachnid, is automated app has repeatedly transmitted a significant amount of content to hotlines around the world.

[978] Marketing & Media Online, The following websites are available from NMHH <https://www.mmonline.hu/cikk/szuloknek-keszit-weboldalt-az-nmhh/> accessed 30 July 2020.

On the 1 March 2020, NMHH launched a website addressing parents at the address www.gyerekanaten.hu and explaining about the many oddities their children talk about in the context of their online experiences in the form of short, clear articles. To get to know the site, and also in connection with this year's theme of Safer Internet Day, the online identity, NMHH created a 15-second video. In it, they unfurl a girl's social media photo, while behind the distinctive settings, filters and stickers, a real child emerges.

The creators use this to show the distance that is almost naturally created on social media between online and real identity. The NMHH advises parents to talk to their children about what they create based on their online appearance and how they present themselves online.

Hungary's Digital Child Protection Strategy aims to promote more effective preparation of children, families, communities, NGOs, educational institutions and the state institution system for value-creating Internet use. Digital culture is increasingly influencing our daily lives, society and economy in a decisive way. For citizens of the information society, conscious internet use as a channel of access to digital culture is one of the most important, highly complex capabilities. Conscious, value-creating internet use brings multiplier successes in terms of both individual contacts, quality of life, social relations and the country's competitiveness.

In addition to promoting conscious, value-creating internet use, the strategy's main objective is to identify and assess the threats and risks to children in internet use, to reduce as much as possible harmful effects, and to eliminate the problem. The strategy addresses the need to provide the knowledge, and acquisition necessary before entering the online space to ensure the conditions for safe internet use.

The strategy builds on the results of government programmes on similar subjects in previous years, in particular the achievements of the first (2012) and the second (2013) Child-Friendly Justice Bill.

Children are at the heart of the strategy, but with it almost all groups in society can be considered concerned; persons closely connected to children (parents, educators), the state institutional system, industry players and NGOs operating in this area. The information society is primarily a networking society; intergenerational cooperation, mutual knowledge sharing and teaching, and bringing together different actors in society are essential for success.[979]

[979] Government of Hungary, Hungarian Digital Wellbeing Program - Digital Child Protection.

A high level of education for children as an objective also involves training the teaching base. As a starting point, the assessment of the current state cannot be avoided, since in the absence of adequate data and information, the tasks that are necessary cannot be carried out with full efficiency.

The objective set by the strategy is to ensure that the available protection mechanisms are properly and efficiently functioning. The path to this does not lead primarily through the establishment of further legal prohibitions; in this respect, the legal system has largely reached where it can go, i.e. widespread restrictions and prohibitions seek to ensure the online safety of children. As the legal system stands, only minor corrections are required, not the legalisation of new criminal practices or restrictive measures. The effectiveness of the restrictions can be achieved in part through the continuous monitoring and development of available technical solutions, with a key role for representatives of the telecommunications industry and partly through the monitoring and development of available technical solutions, prepared for children by producing content and by creating appropriate internet interfaces through which they can acquire the necessary knowledge and experience according to their maturity level.

7.2 Notification-removal procedures

The notification-removal process means that someone notifies the hosting provider of infringing content or information, which in this case removes the relevant content. In the case of the e-commerce directive in place in Article 14(1) and (2), the legal basis for the introduction of those proceedings is not covered by the provisions of Article 10 of Regulation (EC) No 1258/2001.

As set out in recital 46 of the E-Commerce Directive, the removal of content or the termination of access should be carried out taking into account the principle of freedom of expression and the procedures laid down at national level for this purpose; the Directive shall be without prejudice to the possibility for Member States to lay down specific requirements which must be complied with without delay before the removal of the data or the cessation of access to it. Accordingly, the Directive does not require the mandatory introduction of notification-removal procedures, but entrusts it to the discretion of the Member States, which is a serious problem as to when the service provider is deemed to be properly informed and what acts it needs to carry out in order to ensure full safe harbour. According to the Commission's working document, the results of the social consultation show that the divergence of Member States' regulations has led to fragmented rules in the Member States, including the content and form of the notification, the timing of removal, the liability for unsubstantiated

notifications and the assessment of when the content can be considered infringing.

Once the notice of removal has been received, the recipient may object to the removal of the information concerned in a private document or authentic instrument of full probative value within eight days. The objection shall include the identification of information removed or inaccessible, including the network address where it was previously available, the information identifying the recipient concerned and a reasoned declaration that, that the information provided by the user does not prejudice the right of the holder to be notified.

Upon receipt of the objection, the holder shall become aware of the users' or their contact details and will be able to take the necessary steps to enforce the claim. The holder has ten working days to enforce their claim for disqualification by order of payment, an action or a criminal complaint.

In view of the notification-removal procedure, the Hungarian rules exempt the hosting service provider from the recipient for damage caused by the removal if, when uninstalling or granting access, they acted in accordance with the law and in good faith. With regard to notification and removal procedures, the Community legislature shall encourage the development of codes of conduct based on self-regulation at a level which contribute to the protection of intellectual property rights. As voluntary regulation has been confirmed in a decade, the European Commission issued a factsheet in early 2012 on rules on the single digital market for e-commerce and online services based on the plans to establish uniform rules on notification and removal procedures in the future. In this context, social consultation has also been initiated at European level, the results are currently being agitated.

7.3 Liability of internet intermediaries

The responsibility of the broadcaster and intermediary service provider for the transmission of media services and press products is regulated in Act. No. CLXXXV of 2010. on media services and mass communication: '§ 188 * (1) The broadcaster may, under § 189, be obliged to suspend or terminate the transmission of media services in an official decision issued by the Media Council under official authority.'

The intermediary service provider shall, in the Article 189, take the information referred to in Article 189(1) and (2). According to section 10, the media service and the communication of the internet press product may be suspended in the official decision of the Media Council issued under official authority.

In the Agreement on the European Economic Area and in the 1998 Agreement, the European Economic Area agreement was amended by Decision of the European Economic Area to be incorporated into the Agreement. The commission shall, in the first place, take into Law on cross-border television in Strasbourg, 1989. The broadcaster shall not be liable for the content of the broadcasting programme of a broadcaster under the jurisdiction of a State which is not covered by the European Convention and its Additional Protocol. Article 189 shall be a good time for the following: 176-180, taking into account the fact that the information provided for in Articles 176 to 180 is not available. However, it may be required to suspend the distribution of the media service in an official decision issued by the Media Council under official authority.

7.3.1. Types of intermediary service providers[980]

In the online world, there are many types of intermediary service providers. Since e-commerce is constantly and continuously evolving, it is not possible and should not define the concept of intermediary service provider, since any conceptual experiment would violate the requirement of technological neutrality. It should be noted here that many online service providers can simultaneously provide a number of services, even subject to different regulatory regimes, which directly affects their liability for the activity. Thus, on the one hand, an intermediary service provider may act as a content provider (as an online newspaper) for which it is directly responsible for services, whereas, on the other hand, blogs or online forums belonging to the online newspaper the same approach is followed by the case law of the Court of Justice of the European Union.

The regulatory regime for each intermediary service provider is therefore the basis for the activities of the service provider, which may act in the roles set out below. The network provider or access provider under harmonised rules, the provider shall not be liable for the content of the information transmitted.

The responsibility of intermediary service providers and the monitoring of their services are a serious development area, which, by virtue of the fact being, is also directly influenced by developments in European Union law. The practice and legal role of the Court of Justice of the European Union have a special role in this, as the E-Commerce Directive (2000) and the Intellectual Property Rights Enforcement Directive (2004) at a time when digital infringements have not yet occurred at a mass level, as at the present level.

980 Ádám Liber Dr.: Liability of intermediary service provider for intellectual property infringement in the European Union, 2013 <https://www.sztnh.gov.hu/kiadv/ipsz/201303-pdf/01.pdf>-.

The purpose of the legislation cannot be to introduce internet censorship, the identification and tracking of private lysis entities, since these measures are clearly not proportionate to the objective pursued, intellectual property Protection.

7.3.2. Liability of intermediary service providers[981]

As anonymous/pseudonym posts are still most prevalent on the Internet and the identification of the people who create content posted in this way is in most cases obstacles, it is self-evident for the injured parties to try to assert their claim through intermediary service providers.

Only in recent years has the Directive started to provoke debates. But the so-called 'blacklist' of the so-called web2.0 services have been on the Internet for more than 10 years, but only in the last few years have the proliferation of enforcement through intermediary service providers.

On web2.0 interfaces, users create or publish content themselves, and the portal provides technical frameworks for them to appear. The central question is whether these sites are involved in shaping, editing or merely passively playing a passive role and only providing technical support. While it is clear that the activities of these websites constitute a hosting service, it no longer provides a clear explanation as to whether the activities of such websites entitle them to hosting service providers. Thus, it was up to the law to decide on the matter. Under *Delfi A.S. v. Estonia*, it appears that the application of the law, at least for the time being, has voted in favour of the fact that 'web-astwo' providers are not eligible for hosting service providers protection. Although the Decision of the Grand Chamber is still due at the time of writing the sit-down, the Estonian judiciary and the ECtHR have approached the issue similarly, foreshadowing a possible European trend in the issue.

7.4 Blocking and other technical based measures[982]

Today, the technical conditions for blocking have allowed service providers to close routes that allow copyright infringements in the digital space to be blocked in order to exempt themselves and users. This task is not only blocked, but other technical measures are also available, since the development of information technology has not only resulted in the flow of information and file sharing, but also inspired a series of innovations protection against infringements. It has

[981] János Ancsin: Freedom of expression on the Internet, with particular reference to the liability of intermediary service providers, 2013.

[982] István Harkai, Denied Access - blocking websites as a possible means of enforcement, 2016.

generated a kind of 'space competition', as rightholders have recognised that not only is the now outdated toolkit of law, but also rapidly evolving.

Blocking content available on the Internet not only enriched copyright edits, but also allowed restrictions on access to unwanted content in a number of other cases, both individual and public interest. Websites that transmit content to the public may be grouped according to whether they are specifically designed to facilitate the infringement or operate basically lawfully but can be found undesired content. Also, that the file sharing, its although illegal works account for the bulk of the data traffic, it can also be used for legal sharing in many cases, which are unreachable and that is a concern. The history of blocking, which has been written for nearly 20 years, has evolved into a number of variations. These include simple block-up staunch and filtering; mechanisms that providers can use as a temporary measure; content restriction and filtering at the institutional level; particularly against politically harmful content.

The requirement set by the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Infosoc) and Enforcement Directives has added to the expectations of the TRIPS Agreement, which has been transposed into EU law, making it more precise. The TRIPS Agreement, which came into effect on 1 January 1995, is to date the most comprehensive multilateral agreement on intellectual property. The agreement envisages an immediate and effective procedure for infringements of intellectual property rights. However, among provisional measures, it only names the presentation of reasonable evidence, the security or the equivalent guarantee.

The so-called 'block-up orders' are a 'long-imposed' notice and block, meaning that the provider must be aware of the underlying infringement and the properties of the website you want to block, including the IP address and URL. This is necessary so that the provider can also block the IP address and URL of the website that is attacked.

Each website operated by a server has a unique address, the Internet protocol address. Each service provider has at its disposal a database called the 'database'. DNS (Domain Name System), which contains IP addresses and associated domain names. When a user wants to connect to a specific web page, the domain name is converted to an IP address by the provider's DNS system.

There are technically several methods for blocking:

— You can delete or change the IP address of the website that is attacked from your DNS system.

— Service providers can also use a network device, namely the router, to block IP addresses.
— When blocking URLs, service providers are reporting traffic. Data traffic may be collected in the so-called 'data traffic' deep packet inspection, which checks the content you want to view by keyword and then blocks it by keywords on the block list.
— Some service providers use a so-called two-stage system. In the first stage, the IP address is diverted and URLs are blocked in the second stage.

If the user wants to connect to a page in the first step with blocked content, the second step takes effect, which means that the user's request is hijacked. In the second step, traffic that connects to the blocked URL or IP address is stopped. For the method used in both of the third and fourth options, so-called proxy.

Even more problematic – and not only for blocking, but also for notice and takedown – is that the servers of the websites attacked are simply moved to another country by operators. Copyright is protected in most countries of the world, which can multiply jurisdiction, especially if the infringement takes place in several countries, one of which is outside the European Economic Area. The situation of right holders is less disadvantaged if we take into account only the region of the world where the relevant European Union standards apply. These set a clear framework for both the enforcement of intellectual property rights and civil litigation.

It is also important to investigate this issue because several service providers can operate in a given jurisdiction or a service provider may be present in multiple countries. If the latter situation exists, it is possible that the website attacked will be blocked in several countries at the same time. However, if the measure takes place in only one country, the content will remain easily accessible from another country, even in neighbouring countries.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

'Expression is partly the possibility of expressing the speaker's self-expression and his personality freely. According to the individual justification of Freedom

of Expression, the Right to Communication is not only supported by its consequences, but by the moral right of everyone to say what it wants.'[983]

As regards expression as a means of public opinion, article 30/1992 does not apply. (V. 26) Constitutional Court decision lays down the basic principles that 'the Right to Free Expression is, as mentioned above, not only a fundamental subject right, but also an acknowledgement of the objective, institutional side of that Right as a guarantee of public opinion as a fundamental political institution'. This decision, although it is quoted, first and foremost, by Hungarian jurisprudence, is indeed about much more, about the desirable image, conditions, elements and burdens of the democratic public,[984] thus offering points related to non-legal aspects of our subject:

'Expression of opinion in this approach is therefore the instrument that operates the social public and ensures the conditions for the individual's well-founded opinion and democratic participation (instrumental justification) by publicly collating opinions.'[985]

8.1 Aims of the Hungarian Campaign

The campaign is acting on the mobilisation of young people and combating hate speech, who represent and promote human rights culture and democratic citizenship online and offline. The campaign's goals are detailed:

- Raising awareness and raising awareness of hate speech online and offline;
- Support human rights education activities to combat hate speech, raise awareness of the consequences of hate speech and improve the well-being of young people;
- Tools and mechanisms for reporting hate speech, in particular online hate speech;
- Development and dissemination at European and national level.
- Mobilising national and European partners to prevent and combat hate speech and intolerance that appears online and offline;
- Promoting digital literacy and digital citizenship and supporting young people's participation in internet regulation contribute to the implementation of the Council of Europe Action Plan, which is a counter-terrorism approach to violent cyberbullying and radicalisation,

983 Galik-Polyák, 2005, page 58.
984 Szekely, 2013, page 11.
985 Galik-Polyák, page 58.

in particular by identifying and addressing the causes of violent radicalisation of young people.

The campaign is supported by the Council of Europe and its European partners and is implemented by national campaign committees in the Member States.

The portal of the campaign's leaders at national and European level provides up-to-date information on campaign-related activities and the availability of national campaign committees and campaign coordinators.

The purpose of the online platform is to support the Movement and show the image of the campaign. Personal confessions and manifestations of young people can also be found here. Anyone can register as a user on the website and join the movement. The platform is run by online activists and volunteers. The Hungarian campaign website of the campaign is edited by the Hungarian campaign committee. This interface of the campaign website contains online hate speech cases collected by users. It provides opportunities for dialogue with other young people involved in the campaign on how and by what means to take action in each case, as well as to organise actions against hate speech.

The www.nohatespeechmovement.org page also includes a blog with campaign activists and partners publishing information on initiatives and activities across Europe. You can also discuss current issues related to your campaign or hate speech.

Anyone can join the forum at http://forum.nohatespeechmovement.org address to discuss hate speech online or offline, as well as a number of other topics related to the campaign. The forum is moderated by online activists and volunteers.

Although the main activities take place online, the campaign also has offline events such as trainings, seminars, conferences, youth events, festivals, flashmobs. And, of course, many training activities take place in both formal and non-formal learning environments.

Action days are regular action events that will be organised throughout the campaign, involving activists from both national and European campaigns. Each action day focuses on a specific aspect of hate speech and encourages action to support specific target groups. Action day programs include many different online activities that are coordinated. The dates and themes of the action days are updated regularly on the website.

The videos introduce you to the problem of online hate speech and demonstrate the tools and approach of the No Hate Speech Movement. There are several videos on the campaign's main website.

The Guide helps Internet users understand the human rights that apply online, their possible limitations, and the means of redress that are available and applicable to such restrictions.

9. How do you rank the access to freedom of expression online in your country?

According to the prevailing view, freedom of expression has a positive requirement, in addition to its negative nature (non-interference by the state), i.e. the state must ensure that the individual can exercise this right in some form. This was stated by the Hungarian Constitutional Court as early as 1992, declaring that the Constitution entails 'a state obligation to ensure the conditions for the development and functioning of democratic public opinion'. However, as we will see, the formula is not that simple. With regard to the regulation of the subject matter, it should be noted that although the need for the right to the Internet was already raised in the 2000s, despite the ever-increasing relevance, there has been no constitutional declaration on the subject.

10. How do you overall assess the legal situation in your country regarding internet censorship?

The ministerial justification for the legislation integrating the possibility of blocking, first in the criminal law system, states that 'a number of offences can be committed through an electronic communications network. For example, acts of terrorism, child pornography, racist acts, fraud, copyright infringement, consumer deception, personal data abuse, defamation, defamation, etc. However, there was no legal requirement between the provisions in force to make such illegal content unavailable by the determining authorities. Due to the specific nature of the medium, the general rules of confiscation could not be interpreted. Therefore, in order to remove or prevent access to infringing data published on the electronic communications network, Article 77 of the new Criminal Code. No new measures have been introduced by 1 July 2013. This procedure was finally given the name of the definitive inaccessibility of electronic data.

From 2016, the National Transport Authority (NCA) may block the 2012 Directive on passenger transport services. In the Act of 2004, the Commission the website of service providers for which a licence was imposed for lack of a licence and the fined service provider continued to operate without authorisation. This would have been the 'ultimate weapon' against Uber, but the regulations remained in the legislation without 'sharp deployment' - as a memento.

It is clear that there is no longer any question of the need for the court's involvement in blocking content. The fully autonomous decision of the NCA and NAV is perfectly sufficient to start blocking content. There cannot be found any notices, descriptions or even a factsheet on the NKH's website, which indicated blocking.

However, it was necessary to expand the system not only legally, but also technically. Perhaps many people would not think that KEHTA's foundations were established by Interface Computing Ltd. on behalf of NMHH for just over 7 million forints

With a little exaggeration, a situation could have arisen, as if a Hungarian court could impose a prison sentence without even a single prison in Hungary. On the basis of the public list kept by NAV, it is clear that, for technical reasons, the blocking of many websites has not been implemented or suspended to date. KEHTA's system and capabilities are therefore being expanded. Online Projects Ltd. won the public procurement related to the restructuring of the system with an offer of HUF 39.7 million. Under the new contract, improvements could take until 2018.

Since mid-2014, however, the system for filtering infringing online digital data content is likely to be in operation, so years of experience could give you an opinion on whether or not you have fulfilled your expectations. However, the content of KEHTA can be understood by the text of the legislation, which is partly understandable, since the aim is to ensure that the infringing websites are not accessible.

The examination of the institution is therefore far from simple, but it is considered that it was not impossible, so I appealed to NMHH for a request for data to specify the number of URLs currently blocked in KEHTA and on the item page of the claim,

The Metropolitan Court replied to the request for data that the judges handling international cases had informed me 'that, in their memory, a request for enforcement of the final inaccessibility of electronic data had not been received

by the Metropolitan Tribunal in the last four years. They also said that, given the specific nature of the measure, if such a case had been received, it would have been remembered.'

The Public Prosecutor's Office indicated that the Public Prosecutor's Office had made a motion to make electronic data permanently inaccessible for two defendants. In the case of one of the defendants, Article 219 of the Criminal Code has been used. In the case of the other defendant, the prosecution was prosecuted for the commission of an act of terrorism which violated Section 316 of the Criminal Code of Hungary. No information was collected on the temporary inaccessibility.

In essence, even without the 'involvement' of NMHH, it was found that electronic data had been definitively inaccessible in Hungary until mid-2016. Moreover, none of them were the 'threesome' which brought KEHTA's system to life, i.e. child pornography, state crime or acts of terrorism, but websites were permanently blocked in Hungary on the basis of essentially minor offences.

However, no response was received to the number of times and under what title it has been made in Hungary. The NAIH's response quickly revealed to me that a trial on this issue was already pending, in essence, in line with everything they had in all the allegations launched by the TASZ against NMHH a few months earlier. NAIH was therefore unable to conduct a substantive investigation as a result of my announcement.

Turning to the trials: the court of first instance finally ordered the NMHH to inform the TASZ within 15 days of the number of times it had fixed the obligation to temporarily prevent access to electronic data at the request of criminal courts in criminal cases. In addition, the action was dismissed.

The Metropolitan Court of Justice is a member of the Court of Justice of the Council on 32. Pf.21.122/2016/6. In its judgment of it partially changed the judgment of the Court of First Instance and required the NMHH to communicate within 15 days of the number of cases in which the obligation to temporarily prevent access to electronic data entered into KEHTA was deleted by legal basis until the date of receipt of the data claim.

'The National Media and Communications Authority shall, in the case of the ATO. From the entry into force of Section 92/A to the date on which the data claim was answered (18 May 2017), the obligation to temporarily prevent access to electronic data in the KEHTA has not been fixed at any time at the request of criminal courts.'

This is even more in light of the fact that the introduction of KEHTA – at the beginning of 2014 – was delayed on the basis of a modification of the contract

with Interface Computing Ltd. precisely because OBH was not prepared to integrate the system at the time indicated. On this basis, it is clear that the management systems of KEHTA and OBH operate in a very tight, integrated system.

The current role of KEHTA could hardly be further from the legal policy concept that brought the blocking or otherwise screening system to life.

While a wide range of infringing content is likely to be available as a result of the most serious offences under the original concept (e.g. child pornographic content, financing terrorism in a later regulatory environment) it seems that the legal institution is almost not practiced in criminal proceedings, and when they do, they are more of a minor offence.

The pages mentioned in the policy studies, which the law enforcement court considered Holocaust denier or even infringing copyright, are also available from Hungary without problems or disruption, and even the domestic service providers themselves guarantee rapid recovery in the event of a 'malfunction'.

Overall, it may be colluded that however much our deficits may be, we always try to keep up with the current European trends and hope to become an essential part of it. On Hungarian National level it can be seen that the freedom of speech online is granted, sometimes taken for granted. That is the reason why Hungary already has many legislative acts and European case law. The Internet is free, the majority of the population has access to the World Wide Web, and citizens use info communication technology not only for community purposes and intelligence, but also for political activity. There is no censorship in online media content in Hungary, anyone can start a blog, freedom of expression. The network system is not censored by government-independent information society services, but is controlled by national security services.

Table of legislation

Title of the legal act	**Provision text in English language**
2010. évi CLXXXV. törvény a médiaszolgáltatásokról és a tömegkommunikációról	Act CLXXXV of 2010
Alaptörvény	The Fundamental Law of Hungary (25 April 2011)
1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről	Act XXXVIII of 1996 on International Assistance in Criminal
2014. évi XXII. törvény a reklámadóról	Act XXII of 2014 on the advertisement tax.
2003. évi C. törvény az elektronikus hírközlésről	Act C of 2003 on electronic communication,
2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról	Act CXII of 2011 on data protection and freedom of information,
2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről	Act CXIII of 2011 on home defense, Military of Hungary, and the implementable measures under special legal order

Bibliography

Books and Reports

Andras Gergely, "Hungary Phone Tax Burden May Affect Magyar Telekom Dividend," *Bloomberg Business*, May 10, 2012

Anna Galácz, Ithaka Kht, eds., "A digitalis jövő térképe. A magyar társadalom és az internet. Jelentés a World Internet projekt 2007. évi magyarországi kutatásának eredményeiről," [The map of the digital future. The Hungarian society and the internet. Report on the results of the 2007 World Internet Project's Hungarian research] (Budapest: 2007): 20.

Budapest Internet Exchange (BIX), "BIX Charter," Jan 21, 2019

Digital Transformation of Small and Medium Enterpises in Hungary, DELab UWCountry Report, February 2016

OSCE, "Revised Hungarian media legislation continues to severely limit media pluralism, says OSCE media freedom representative," press release, May 25, 2018.

Privacy International "Surveillance Industry Index," November 18, 2013, https://www.privacyinternational.org/node/403.

Venice Commission, "Opinion on the Fourth Amendment to the Fundamental Law of Hungary," 17 June, 2013, http://bit.ly/1U8x0CD.

Zoltán Kalmár, Council of Hungarian Internet Service Providers, e-mail communication, January 24, 2012.

Internet sources:

"Akcióba lendült a magyar Anonymous" [Hungarian Anonymous in action], 24.hu, May 2, 2017, http://bit.ly/2rqsc25

"Another decision for non-discriminatory internet", [Újabb döntés a megkülönböztetéstől mentes internetezésért], National Media and Infocommunications Authority, January 27, 2017, http://bit.ly/2nMK73V.

"Hungary: Tens of thousands march in Budapest anti-Orban demo", *BBC News,* April 14, 2018, http://www.bbc.com/news/world-europe-43771392

"Lerángatták a lépcsőn a 444 tudósítóját, és elvették a telefonját a Fidesz konzultációs kórumán" [444 reporter dragged down on stairs, her phone taken away], 444.hu, May 5, 2017, http://bit.ly/2q37djV

"Nemzetközi háború a kormány ellen?" [International war on the government?], 24.hu, December 26, 2015, http://bit.ly/2pKJNnZ

"Soros's native Hugnary approves crackdown on foreign funded NGOs," *Bloomberg,* June 13, 2017, https://www.bloomberg.com/news/articles/2017-06-13/soros-s-native-hungary-approves-crackdown-on-foreign-funded-ngos.

"The NMHH decided for the non-discriminatory internet", [A megkülönböztetéstől mentes internetezésért hozott döntést az NMHH], National Media and Infocommunications Authority, December 1, 2016, http://bit.ly/2mzR2xF.

„Nem titkolják tovább, Mészáros Lőrinc az Opimus tulajdonosa" [It is not a secret anyomore: Opimus is owned by Lőrinc Mészáros], *hvg.hu,* March 3, 2017, http://bit.ly/2oda6hn.

Ádám Lestyánszky, „The Budapest Beacon exit interview". *Budapest Beacon,* April 13, 2018, https://bit.ly/2JIMA7Q

Ágnes Urbán, Attila Bátorfy, "State advertising in Hungary 2006-2017," [Állami hirdetések Magyarországon, 2006-2017], *Mérték Media Monitor,* February 23, 2018, http://bit.ly/2ossB3l

András Dezső-Szabolcs Panyi, *„We Are Not Paid Agents of Russia, We Do It out of Conviction"*, Index.hu, 30 January, 2017, http://bit.ly/2nkkxCq.

Anita Vorák, "Így kaptak Tiborczék szabad utat a milliárdokhoz", [This is how Tiborcz and his crew gained access to the billions], 444.hu, 11 March, 2015,

Anita Vorák, „Six things Direkt36 revealed the company of Orbán's son-in-law, and later were also found suspicious by the EU'S Anti-fraud Office," *Direkt36,* February 14, 2018, http://bit.ly/2okPt5k

Attila Bátorfy, journalist of Kreativ.hu, authored an in-depth analysis of public funds moving to private hands via media advertisements between 2010–2014: "Hogyan működött Orbán és Simicska médiabirodalma?" [How did the media empire of Orbán and Simicska work?] *Kreativ,* February 18, 2014, accessed March 7, 2015, http://bit.ly/1EZM9yM.

Attila Kálmán, „It is the videojournalist of 444 who has to go to court, not the Fidesz member," [A 444 videósa áll bíróság elé, nem a Fidesz-tag], *24.hu,* 24 October, 2017, http://bit.ly/2ELK6q7

Attila Mong, et al, „When Propaganda Rules Public Discourse – Soft Censorship in Hungary 2016," *Mérték Média Monitor, page* 55, http://bit.ly/2Cf0EVQ

Attila Mong, et al, „When Propaganda Rules Public Discourse – Soft Censorship in Hungary 2016," *Mérték Média Monitor, page* 55, http://bit.ly/2Cf0EVQ

Daniel Nolan, Shaun Walker, „Hungarian journalists admit role in forging anti-migrant atmosphere of fear"', *The Guardian,* April 13, 2018, https://bit.ly/2qvx7yT

European Commission, "State aid: Commission opens in-depth investigation into Hungarian advertisement tax," March 12, 2015, http://bit.ly/1b5b88P.

European Schoolnet and University of Liege, "Survey of schools: ICT in education, Country profile: Hungary," November 2012, http://bit.ly/1IVN56J.

Facebook-perek sora kezdődhet a súlyos joghézag miatt" [Many Facebook-related lawsuits may be initiated due to legal loophole], *mno.hu*, February 3, 2016, http://bit.ly/2esv9cD.38

Gergő Plankó: "Húsz éven át építették, a lakájmédia konca lett" – itt a teljes levél arról, mi lett az Origóból, [It was being built for 20 years, today it is the prey of government propaganda – here is the full letter about the faith of Origo], 444.hu, 11 March, 2017, http://bit.ly/2nW2Jzy

http://bit.ly/1T67rmA.

http://bloom.bg/1G2ceQG.

https://444.hu/2018/01/30/a-fidesz-egyik-facebook-katonaja-elmeselte-milyen-virtualis-hadsereget-hozott-letre-a-part

https://ataszjelenti.blog.hu/2018/03/23/velemenyt_mondani_marpedig_szabad

https://bbj.hu/business/digi-to-launch-hungarian-mobile-services-in-june-after-delay_144025

https://bit.ly/2KhXotV

https://hvg.hu/itthon/20180828_Buszken_vallja_a_TASZ_hogy_nem_fogad_el_allami_vagy_onkormanyzati_adomanyt_most_kozvetve_megis_ilyen_penz_jutott_hozza

https://rsf.org/en/news/one-hungarys-last-critical-media-outlets-taken-over-orban-allies

https://szabadindex.eu/

https://www.reuters.com/article/us-hungary-election/hungarys-strongman-viktor-orban-wins-third-term-in-power-idUSKBN1HE0UC

https://www.reuters.com/article/us-hungary-media-index/businessman-sells-company-with-indirect-control-over-hungarys-main-independent-news-website-idUSKCN1LX2DE

https://www.theguardian.com/world/2016/oct/01/hungarian-referendum-slam-...

Hungarian court blocks Holocaus denial websites," *Times of Israel*, September 1, 2016, http://www.timesofisrael.com/hungarian-court-blocks-holocaust-denial-websites/.

Hungarian opposition daily Magyar Nemzet to shut down", *Business Insider*, April 10, 2018, https://read.bi/2I09RBA

Így hazudik az Origo: a 2017-es európai migránstámadás egy 2015-ös amerikai rablás", [This is how Origo lies: the 2017 European migrant attack is a 2015 American robbery], hvg.hu, March 14, 2018, https://bit.ly/2IrFhzD

Imre Fónai, "Facebook-per:a siófoki expolgármester nem hagyja annyiban" [Facebook trial: Siófok ex-Mayor will not give up], *sonline.hu*, June 23, 2016, http://bit.ly/2dz6t3C.

József Spirk, "Egy ügyvédet lehallgattak, a többiek csak a jeleit észlelték" [Attorney tapped, others suspect the same], *index.hu* April 21, 2016, http://bit.ly/2drjUk8.

Justin Spike, „Fidesz-tied oligarchs now control all 18 regional newspapers," *The Budapest Beacon, August 5, 2017, http://bit.ly/2CF4VxM*

László Szily, "Sima Facebook-megosztásért hallgattak ki és rabosítottak 17 embert Diófokon" [17 people interrogated and fingerprinted for a Facebook share], *444.hu*, November 27, 2015, http://bit.ly/2cYf4Mx.

László Tamás Papp-Babett Oroszi, *"Nemzeti radikális hírportálok: Oroszország magyar hangjai"*, [National Radical Newsportals: The Hungarian Voice of Russia], Atlatszo.hu, 26 August, 2014, http://bit.ly/2nLX4e9

Lili Bayer, „Brussels launches infringement proceedings against Hungary," *Politico.eu,* July 13, 2017, http://politi.co/2olCPTH

Lóránt Győri et al, "Does Russia interfere in Czech, Austrian and Hungarian elections?", 2017, p 12, https://bit.ly/2zhV6oZ

Marton Dunai, „Orban re-election campaign may be undercut by tactical voting", *Reuters*, April 4, 2018, https://reut.rs/2r1tuB4

Máté Dániel Szabó: *„What is Szilárd Németh using the secret services for?"*, [Mire használja Németh Szilárd a titkosszolgálatokat?], ataszjelenti.blog.hu, March 14, 2016, http://bit.ly/2nlqM98

Max Bearak, „Hungary accused of 'hatemongering' in national survey targeting George Soros," *The Washington Post,* November 8, 2017, http://wapo.st/2GEjUdR

Mérték Médiaelemző Műjhely, Publicus Research, *"Médiamenedzserek a sajtószabadságról",* [Media managers on the Freedom of the Press], page 7, http://mertek.eu/wp-content/uploads/2016/07/mediamenedzser2016.07.18.pdf

Morgan Marquis-Boireet. al. "For their eyes only: The Commercialization of Digital Spying," Citizen Lab, September 16, 2013, http://bit.ly/1pCA0Y4.

Pablo Gorondi, "Hungary: Pro-govt weekly prints list of 'Soros mercenaries'", *Associated Press,* April 12, 2018, https://www.bostonglobe.com/business/2018/04/12/hungary-pro-govt-weekly-prints-list-soros-mercenaries/858ycSqJO03tzRYY6Qvg4O/story.html

Palko Karasz, „Hungary's Parliament Passes Law Targeting George Soros's University", The New York Times, April 4, 2017, http://nyti.ms/2o8EH36

Péter Erdélyi, Péter Magyari, Gergő Plankó,"Deutsche Telekom, Hungarian government collude to silence independent media," 444, June 5, 2014, http://bit.ly/1hClHm6.

Péter Erdélyi, Péter Magyari, Gergő Plankó,"Deutsche Telekom, Hungarian government collude to silence independent media," *444*, June 5, 2014, http://bit.ly/1hClHm6.

Pricewaterhouse Cooper, "Changing advertising tax rates," May 27, 2015, http://pwc.to/1MEwHKp.

Sándor Czinkóczi, „All of the county papers published the same centralized Orban interview a day before the elections" [Az összes megyei lap ugyanazzal a központi Orbán-interjúval jelent meg a választás előtti napon], *444.hu,* April 7, 2018, https://bit.ly/2I19WqU

Tamás Bodoky, "Nem cask az USA szeme látmindent: kormányzati kémprogram Magyarországon," [Not only USA can see everything: governmental surveillance software in Hungary] *atlatszo.hu*, September 16, 2013, http://bit.ly/1FWperq.

Tamás Papós, "Esélytelen diákok és 1 Mbit-es internet a magyar iskolákban," [A chance for students and 1Mbit internet at Hungarian schools] *Hvg.hu*, October 3, 2013, http://bit.ly/1RxESuy.

Telefonadó: A Telenor és a Magyar Telekom is emeli a díjait," [Telephone tax: both Telenor and Magyar Telekom raises prices] *Hvg.hu*, September 10, 2013, http://hvg.hu/gazdasag/20130910_Vandorlasba_kezdhet_a_mobilpiac.

Viktória Serdült, "Prosecutor orders investigation into surveillance bug found in NGO office," *The Budapest Beacon*, July 14, 2016, http://bit.ly/2cOhJoE.

Zsófia Gergely, "Megszólalnak a bírók: jobbelugrani a kényesügyelől", [The judges speak up: it is better to avoid politically sensitive cases], *Hvg.hu*, 1 March 2016, http://bit.ly/1QR84Ah.

Periodicals:

TNS-Hoffmann Kft. Media Sector TGI 2014/1–4 quarters.

Alex Hern, "Hacking Team hack casts spotlight on murky world of state surveillance", *The Guardian*, July 11, 2015, http://bit.ly/2efzrIq.

The Hungarian Helsinki Committee, "Bill seeks to stifle independent groups," June 12, 2017, http://www.helsinki.hu/en/hungary-bill-seeks-to-stifle-independent-groups/.

Case Law:

Case C-288/12, Commission v Hungary, April 8, 2014.

Eötvös Károly Policy Institute, "Szabo and Vissy v. Hungary: No secret surveillance without judicial warrant," http://bit.ly/1Bh3uhu;

European Commission vs. Hungary, Case C-462/12, November 22, 2013; and "EC drops suit over Hungary telecoms tax," *Politics*, September 27, 2013, http://bit.ly/1QdD20V.

Magyar Jeti Zrt. v. Hungary, Application no. 11257/16. Many prominent internet stakeholders intervened in the case, such as Mozilla or Buzz-feed: http://hudoc.echr.coe.int/eng?i=001-164079.

Magyar Tartalmoszolgáltatók Egyesülete and Index.hu Zrt. v. Hungary, (application no. 22947/13).

Pfv.IV.20.011/2015/3, June 10, 2015.

Szabó and Vissy v. Hungary, Application no, 37138/14., 14 January 2016.

NAIH-4991-9/2012/H Pesterzsébet; Disclosure of documents related to funeral assistance, *NAIH-5951-16/2012/H.* Data management of Generál Média Publishing Kft.

ELSA Ireland

Contributors

National Coordinator

Jodie McStay

National Researchers

Eithne Kavanagh

Mary McNicholas

Aifric O'Reilly

Natasha Richardson

Isabelle Naughton

Celeste Cannon

Sean Quinn

National Technical Editors

Liam Sunner

Lisa Boylan

Acknowledgements

I would like to extend my appreciation and thanks to each and every member of this research group for both their individual and group efforts in making this report a success, Aifric O'Reilly, Celeste Cannon, Eithne Kavanagh, Isabelle Naughton, Mary McNicholas, Natasha Richardson and Seán Quinn.

I would also like to express on behalf of myself and the group, a heartfelt thanks to our editing team members Mr. Liam Sunner and Ms. Lisa Boylan. It should be noted that an outstanding amount of time and effort in difficult circumstances was expended in supporting and guiding our group from the beginning of this project through to its completion.

I would also like to extend a special thanks to the ELSA International team for their continuous help and support throughout this project. With particular thanks to Sarah Ikast Kristoffersen, Nikola Ćirić and Fani Dimoska.

Without the above, this project would not have been possible.

Thank you all.

Jodie McStay

National Coordinator, ELSA Ireland.

May 2020

Introduction

The aim of our National Research Group is to examine the Irish legal stance on Internet Censorship and in particular the balance between the right to freedom of expression online and the protection of privacy, IP-rights, legitimacy of information, and the regulation of hate speech. This will be achieved through an exploration of both private and public regulations, while addressing the legal consequences of enforcing takedown or deletion procedures.

Overall, we will find how Ireland performs in balancing online regulation of material and the protection of rights such as freedom of expression, the right to privacy, and the right to be forgotten amongst others. Striking a balance between safeguarding and surveillance is difficult as there exists a myriad of aspects that need to be taken into consideration.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

There is a Constitutional right to freedom of expression in Ireland as laid out in Article 40.6.1(i) of Bunreacht Na hÉireann[986] (Hereinafter referred to as the Constitution). There are, however, some limitations on your freedom of expression. For example, the Censorship of Publications Acts[987] and the Censorship of Films Act 1923 allows for the censorship of publications such as books, films, and DVDs. There is also the Defamation Act 2009 that places limitations on the freedom of expression in relation to the protection of one's good name and reputation. The freedom of expression is carefully balanced with the right to one's good name[988] and the right to privacy. While not explicitly stated in the Constitution, the right to privacy is given common law recognition by implication from the Constitution's personal rights provisions.[989]

The right to privacy was first recognised in Ireland by the Supreme Court in McGee v Attorney General.[990] In this case, a statutory ban[991] on the importation of contraceptives to Ireland was overturned. Walsh J. held that Article 41 of the Constitution guaranteed a husband and wife protection against the invasion of

986 Bunreacht Na hÉireann 1937.
987 Censorship of Publications Act 1929; Censorship of Publications Act 1946.
988 Article 40.3.2 of Bunreacht Na hÉireann 1937.
989 Ibid (n 1), Art 40.
990 [1974] IR 284.
991 Criminal Law Amendment Act 1935, s 17.

their privacy by the State in respect of contraceptive choices.[992] In the subsequent Supreme Court case of Kennedy and Arnold v Attorney General,[993] Hamilton P held that the right to privacy was one of the unenumerated rights recognised by Article 40.3 of the Constitution. In this case it was held that an individual's written and telephone communications may not be 'deliberately, consciously, or unjustifiably'[994] interfered with. However, no constitutional right is absolute. Interference with the right to privacy is permissible and may be justified in the interest of the common good, morality, and public order.[995]

Ireland's recognition of the importance of internet safety has grown over the last number of decades. To combat growing safety concerns, Ireland has set up the National Advisory Council for Online Safety (NACOS) as part of the Action Plan for Online Safety 2018-2019.[996] The Council members are drawn from various children's and parents' organisations, major online platforms, and experts in the field of online safety issues. While the Advisory Council has no legislative powers, they are a body producing detailed and publicly available reports. These reports are helpful guides for the Government containing recommendations going forward on how to tackle emerging online including those relating to freedom of expression.[997]

A more recent update with respect to Irish online safety regulations has come in the form of the Government approved Online Safety and Media Regulation Bill 2019.[998] This has led to the commencement of detailed drafting of legislation by the Office of the Attorney General. The proposed legislation is hoped to make a significant difference in tackling the spread of harmful content expressed online. 'The new law is one of the first of its kind [. . .] seen as a critical step in making the internet a safer place, particularly for children.'[999]

In January 2020, the National Advisory Council for Online Safety updated the publication of their legislative documents including the General Scheme of the

992 [1974] IR 284.
993 [1987] IR 587.
994 ibid 593 (Hamilton P).
995 Art 40.6.1 of Bunreacht Na hÉireann 1937.
996 Department for Communications, Climate Action & Environment, 'The Action Plan for Online Safety 2018-2019' (The Government of Ireland 2019). http://www.justice.ie/en/JELR/Action_Plan_for_Online_Safety_2018-2019.pdf/Files/Action_Plan_for_Online_Safety_2018-2019.pdf accessed 20 February 2020. (Action Plan).
997 Art 40.6.1.(i) of Bunreacht Na hÉireann 1937.
998 General Scheme of the Online Safety & Media Regulation Bill 2019 <https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx> accessed 12 February 2020. (Media Bill 2019)
999 '7 things you need to know about the proposed Online Safety and Media Regulation Bill' (PWC, 29 January 2020) <https://www.pwc.ie/services/consulting/insights/7-things-to-know-about-online-safety-media-regulation-bill.html> accessed 20 April 2020.

Online Safety & Media Regulation Bill 2019. This suggests that Ireland is growing and adapting in terms of composing a statutory framework for the necessary measures in tackling the ever-growing issues that relate to online safety and regulating for the protection of freedom of expression.

Ireland has the Censorship of Publications Act 1929, but the Act contains no definition of censorship.[1000] It is arguably an act of some antiquity which could not have envisaged the huge technological advances present within society today in relation to the internet. There is also the Censorship of Publications Act 1946 wherein again there is no definition of censorship. Ireland also has a series of Data Protection Acts from 1988-2018, the purposes of which are to provide a legislative framework to protect people's privacy in terms of personal data and, in addition to this, places responsibilities on the holder of that personal data with respect to its use. Arguably, in turn, this responsibility limits the freedom of expression of holders of such data in how they may utilise it.

Going back to the more recent General Scheme of the Online Safety & Media Regulation Bill 2019, it can be seen there is extensive engagement with online safety, but again there is no mention or definition of censorship anywhere within the Act. The language Ireland is seen to use within the aforementioned legislation is that of 'protection', 'safety, 'privacy' and 'online safety' when referring to harmful online activities. Presumably, from this it may be concluded that issues will remain in balancing the freedom of expression against the protections it is hoped will materialise.

Defined by of Article 19 of the International Covenant on Civil and Political Rights 1966,[1001] the freedom of expression includes the right to receive and impart information. Ireland has enacted the Freedom of Information Act 2014, whereby members of the public have the right to access information and records held by Government departments, local authorities, or public bodies in relation to their duties and roles as well as information held specific to or affecting the individual. The 2014 Act aligns with this Article of the Covenant in enabling the freedom of expression by facilitating the receiving and imparting of information. The Act can also be used to amend incorrect information held about individuals. Mostly, the Freedom of Information Act is used for obtaining records. However, this must be balanced with public interest where records are disclosed, and the right to privacy whereby the records can be withheld or redacted. Part 4 of the 2014 Act entails a long list of exemptions outlining specific circumstances under

[1000] Section 2 of the Censorship of Publications Act 1929.

[1001] United Nations General Assembly Resolution 2200A (XXI) 16 December 1966, in force from 23 March 1976.

which the requested information may not be released. Included under this heading are things such as a threat to National Security, records afforded legal privilege, records obtained in confidence, or if the records that have been requested simply do not exist.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

While there is currently no specific legal framework governing the blocking and takedown of internet content per say, that does not mean there is no scope to do so. As will be discussed in greater detail below in response to question 3, Judges have been willing to expand existing laws when someone's intellectual property rights, good name (and by the same token their finances) are affected in respect to online content.[1002]

The Copyright and Related Rights Act 2000 provides a legal mechanism by which the owner of a copyright may take an action against an infringing party.[1003] Section 127(2) of the 2000 Act sets out the remedies available to a copyright owner which include, but are not limited to, the right to seek an injunction.[1004] Such relief may include an order to remove, desist from sharing, or blocking access to copyrighted material.

Article 8(3) of Directive 2001/29/EC ('Copyright Directive') states that, 'Member States shall ensure that copyright holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'[1005] Article 11 of Directive 2004/48/EC ('IP Enforcement Directive') states similarly in respect of infringements of intellectual property rights, without prejudice to Article 8(3) of the 2001 Directive.[1006] Section 127 of the 2000 Copyright Right and Related Rights Act, Article 8(3) of the 2001 Copyright Directive and Article 8(3) of the 2004 IP Enforcement Directive are read together by Irish Court in determining whether an injunction can be granted against a party who infringes another's copyrights.

1002 Steve Hedley, The Law of Electronic Commerce and The Internet in The UK and Ireland (Cavendish 2006).

1003 Copyright and Related Rights Act 2000, s 127.

1004 ibid, section 127(2).

1005 2001/29/EC Council Directive on the harmonization of certain aspects of copyright and related rights in the information society [2001] OJ L167/10, Article 8(3).

1006 2004/48/EC Council Directive on the enforcement of intellectual property rights [2004] OJ L195/16, Article 11.

In the recent case of The Football Association Premier League Ltd v Eircom Ltd t/a Eir & Ors,[1007] The Irish High Court granted injunctive relief ordering a defendant intermediary service provider ('ISP') to block the unauthorised streaming of Premier League football. In this case, the Court specifically referred to Article 11 of the IP Enforcement Directive[1008] and Article 8(3) of the Copyright Directive[1009] in reaching its decision to grant the relief sought. The Court also referred to the 2016 Court of Appeal judgment in Sony Music Entertainment (Ireland) Ltd & Ors v UPC Communications Ireland Ltd as binding precedent. [1010]

The Sony case concerned an appeal of a High Court order that the ISP implement a form of GRS (Graduated Response Strategy) for the benefit of three named music companies. The term GRS refers to steps which an ISP is required to take against copyright infringers which range from a warning letter to blocking access to specific websites for commercial users. The ISP in question argued that the High Court had no jurisdiction to grant such injunctive relief against them,[1011] a non-infringing ISP by virtue of the defences provided under Articles 12 and 14 of the E-Commerce Directive.[1012] Further, they argued that such an order was more appropriate to a specialist regulator.[1013]

The Court of Appeal dismissed the appeal with Judge Hogan holding that the EU legislator had vested the jurisdiction to grant an injunction against non-infringing parties, or innocent conduits, in the national courts of the Member States by enacting Article 8(3) of the 2001 Directive.[1014]

The key difference between the Sony Music and Premier League cases is that in the former, an order was granted against an ISP to facilitate the blocking of specific end-users from streaming and downloading copyrighted material whereas, in the latter, an order was made against ISPs to block certain websites which facilitated the streaming or downloading of copyrighted material by end-users. This subtle distinction represents a significant development in the law on

---

1007 The Football Association Premier League Ltd v Eircom Ltd t/a Eir & Ors [2019] IEHC 615.

1008 2004/48/EC Council Directive on the enforcement of intellectual property rights [2004] OJ L195/16, Article 11.

1009 2001/29/EC Council Directive on the harmonization of certain aspects of copyright and related rights in the information society [2001] OJ L167/10, Article 8(3).

1010 Sony Music Entertainment (Ireland) Ltd & Ors v UPC Communications Ireland Ltd [2016] IECA 231.

1011 ibid, Hogan J, 4.

1012 Directive 2000/31/EC of the European Parliament and of the Council 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on Electronic Commerce'), [2000], OJ L 178/1.

1013 Sony Music Entertainment (Ireland) Ltd & Ors v UPC Communications Ireland Ltd [2016] IECA 231, Hogan J, 4.

1014 ibid, 62.

blocking and take-down procedures in Ireland regarding internet content which infringes copyright.

While the above cases may be cited as an example of judicial creativity, it is also a marked shift from the previous position whereby ISP's could use Articles 12 and 14 of the E-Commerce directive as a shield against litigation.[1015] Along with judgments from the CJEU such as Glawischnig-Piesczek v Facebook Ireland[1016] it may be inferred there is an appetite to increase the responsibilities of online service providers in preventing, removing and blocking online content.

It is likely that in the near future, specific legislation to address the issues of blocking or the taking down of online content will be enacted in this jurisdiction. Ireland has approved the Online Safety and Media Regulation Bill 2019.[1017] While this is still at Bill stage, meaning it is yet to be given legislative force, it proposes to tackle issues in relation to internet content. The planned legislation will oblige online services to comply with online safety codes for the purposes of keeping users safe.[1018] Failure to do so may result in sanctions ranging from a company being issued with a warning, a notice of non-compliance, fined, or blocked in Ireland for persistent violations or non-compliance.[1019] This proposed legislation is in recognition of the growing desire to regulate online content. It is hoped that these proposed measures will introduce accountability with clear expectations for the providers of online services.

Ireland currently lacks an effective complaints procedure and this Bill aims to tackle issues such as requests to have material taken down from an online platform. This proposed legislation would end the self-regulation period by introducing legislative authority to impose sanctions and hold online users accountable for their online materials.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

There is currently no specific legal framework governing the blocking and take-down of internet content in Ireland. Existing legislation, along with principles found in both the common law and equity, have been developed by the Irish

1015 ibid, 27.
1016 C-18/18 - Glawischnig-Piesczek [2019] ECR I-773.
1017 General Scheme of the Online Safety & Media Regulation Bill 2019. https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx accessed 12 February 2020. (Media Bill 2019).
1018 ibid.
1019 ibid.

courts to facilitate the blocking and take-down of internet content which constitutes or contributes to a tort (particularly copyright infringement and defamation).[1020] Soft-law mechanisms have also developed in order to facilitate the take-down or blocking of internet content which constitutes a criminal offence or is otherwise unlawful.[1021]

In the context of copyright infringement, the Irish courts have expressly relied on the provisions of the ECHR and have adhered to the principles set out in the jurisprudence of the European Court of Human Rights ('ECtHR'), although largely by reference to case law of the Court of Justice of the European Union ('CJEU'). In the High Court case of EMI Records (Ireland) Limited et al. v Eircom Limited and BT Communications Ireland Limited,[1022] Charleton J expressly recognised the right to privacy as being an 'unenumerated fundamental right' which is simultaneously protected by Article 40 of the Constitution and guaranteed by Articles 8 and 10 of the ECHR.[1023].In subsequent cases, such as Sony Music and Premier League, the Court did not expressly refer to the ECHR or the jurisprudence of the ECtHR however, the Court did assess the copyright injunctions by reference to fundamental freedoms, albeit through the examination of EU law and the jurisprudence of the CJEU.[1024]

3.1 Defamation

The Defamation Act 2009 comprises the legal framework governing the law on defamation in Ireland. Pursuant to section 33(1) of the 2009 Act, the court may order an interim, interlocutory, or perpetual injunction to prevent the publication, or further publication, of a statement where the court is of the opinion that the statement is defamatory[1025]. The 2009 Act outlines that, 'the tort of defamation is the publication, by any means, of a defamatory statement'[1026] and thus the online publication of a defamatory statement may be remedied by a blocking or removal order. Issues can, however, arise.

In Muwema v Facebook Ireland Ltd,[1027] Binchy J refused to grant an order against Facebook pursuant to section 33(1) of the 2009 Act to remove defamatory material. It was held that the Court was confined to only making

[1020] The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015.
[1021] ibid.
[1022] EMI Records (Ireland) Limited et al. v Eircom Limited and BT Communications Ireland Limited [2005] 4 Irish Reports 148.
[1023] European Convention on Human Rights, Art 8; Art 10.
[1024] Sony Music Entertainment (Ireland) Ltd & Ors v UPC Communications Ireland Ltd [2016] IECA 231.
[1025] Defamation Act 2009 s 33(1).
[1026] ibid, s 6(2).
[1027] Muwema v Facebook Ireland Ltd (No. 1) [2016] IEHC 519.

such an order where it was apparent that there was no defence that was 'reasonably' likely to succeed.[1028] Notably, Binchy J expressed, obiter dictum, his 'unease' at coming to his decision in circumstances where it appeared that, pursuant to the law in Ireland, a victim of defamation may never succeed against an ISP where there is such an all-encompassing defence of innocent publication provided for in Section 27 of the 2009 Act.[1029] Binchy J noted that there may well be situations where the author of the defamatory statement is unidentifiable and in the absence of relief against an ISP, a take-down order may never be a remedy,[1030] especially where content can be spread to other sites so quickly and so easily.

3.2. Internet Content constituting a criminal offence

As noted above in question 2, take-down and blocking procedures for internet content are not formally legislated for in Ireland. This includes content which constitutes a criminal offence. However, there are some soft-law mechanisms in place to permit the blocking and take down of content which runs contrary to Irish statutes.

In 2014, An Garda Síochána entered into a Memorandum of Understanding with UPC (an ISP) whereby UPC agreed to restrict access to domains or URLs which contained child sexual abuse material (CSAM) pursuant to a list drawn up by An Garda Síochána.[1031] In February 2020, a new Memorandum of Understanding was entered into between An Garda Síochána and a number of ISPs (BT Ireland, Eir Ireland, Sky Ireland, Tesco Mobile, Three Ireland and Vodafone Ireland) to block access to Interpol's 1,857 'worst of' websites containing CSAM.[1032] Internet users who try to view illicit material are redirected to An Garda Síochána's[1033] 'stop page' which notifies the user they are attempting to view illicit material.[1034]

1028 ibid, Binchy J 64.

1029 ibid, Binchy J 65.

1030 ibid.

1031 'An Garda Síochána Sign MOU with UPC on the Restriction of Child Sexual Abuse Material Online' <https://www.garda.ie/en/About-Us/Our-Departments/Office-of-Corporate-Communications/Press-Releases/2014/November/An-Garda-Siochana-Sign-MOU-with-UPC-on-the-Restriction-of-Child-Sexual-Abuse-Material-Online.html> accessed 25 February 2020.

1032 Shauna Bowers, 'Almost 2,000 child abuse websites to be blocked under new initiative: Internet users will be redirected to a Garda 'stop' page when trying to view illicit material' Irish Times (Dublin 10 February 2020) <https://www.irishtimes.com/news/crime-and-law/almost-2-000-child-abuse-websites-to-be-blocked-under-new-initiative-1.4168830> accessed 25 February 2020.

1033 An Garda Síochána, the Irish police force.

1034 Shauna Bowers, 'Almost 2,000 child abuse websites to be blocked under new initiative: Internet users will be redirected to a Garda 'stop' page when trying to view illicit material' Irish Times (Dublin 10 February 2020) <https://www.irishtimes.com/news/crime-and-law/almost-2-000-child-abuse-websites-to-be-blocked-under-new-initiative-1.4168830> accessed 25 February 2020.

Additionally, a number of ISPs in Ireland are members of the Internet Service Providers Association of Ireland ('ISPAI'), a not-for-profit trade association, which operates to self-regulate illegal and harmful use of the internet in a manner which has been overseen by the Government since 1998.[1035] The ISPAI has developed an Industry Code of Practice and Ethics ('ISPAI Code') and has established an Internet Hotline Service (hotline.ie) which operates to allow members of the public to report content suspected of constituting a criminal offence, particularly CSAM.[1036]

The requirements set out in the ISPAI Code appear to be largely aspirational as the words 'best endeavours' are used to describe the standard of action to be taken by the Members to ensure services (excluding third party content) do not contain any illegal material, are not used to promote or facilitate any practices which are contrary to Irish law and do not contain material, 'inciting violence, cruelty, racial hatred or prejudice and discrimination of any kind.'[1037] Given that ISPs operate in an industry of self-regulation and that ISPs usually require that customers comply with their own Terms of Use, it is conceivable that content which is not otherwise unlawful may be taken-down/blocked/filtered if it is prescribed as being contrary to an ISP's Terms of Use. Potentially coming into conflict with personal rights outlined previously such as freedom of expression. On this basis that of self-regulation by ISPs (generally incorporated bodies) in Ireland, their decisions to remove or not to remove internet content is not amenable to judicial review which may leave affected parties with very limited and expensive options to vindicate their rights.

The Irish Internet Hotline Service, hotline.ie, provides a forum overseen by the Department of Justice and Equality and in cooperation with An Garda Síochána, for which members of the public can report suspected illegal content.[1038] The grounds upon which online material should be reported to hotline.ie include CSAM, child grooming activities, child sex tourism, child trafficking, sexual exploitation of children, racism, xenophobia, incitement to hatred and financial scams.[1039] It is self-professed by hotline.ie, that their focus is mainly to deal with reports of online content which contravenes the provisions of the Trafficking

---

1035 Internet Service Providers' Association of Ireland, 'The Voice of Online Industry in Ireland' <https://www.ispai.ie/> accessed 25 February 2020.

1036 Hotline.ie, 'Who We Are' <https://www.hotline.ie/about/> accessed 25 February 2020.

1037 Internet Service Providers' Association of Ireland, 'Code of Practice and Ethics', 10 <https://www.ispai.ie/wp-content/uploads/2013/09/Code-of-Practice-and-Ethics.pdf> accessed 25 February 2020.

1038 Hotline.ie, 'Who We Are' <https://www.hotline.ie/about/> accessed 25 February 2020.

1039 ibid, 'Types of Online Content That Should be Reported' <https://www.hotline.ie/about/what-you-can-report/> accessed 25 February 2020.

and Pornography Act 1998.[1040] A report may be made where internet content contravenes the Prohibition of Incitement to Hatred Act 1989.

3.3. Evaluation

Legislation, such as the 2000 Act and the 2009 Act, has been developed and have been interpreted by the Irish courts to allow the blocking/take-down of internet material which is deemed to constitute a tort. In the context of copyright infringement, the Irish courts appear to perform a balancing test between relevant competing rights[1041] and in the context of defamation, the Irish courts have at least assessed the law through the lens of such rights.[1042] In contrast, the blocking/take-down of illegal online content is not legislated for under Irish national law but rather is governed by a system of self-regulation by ISPs, by an understanding of cooperation between An Garda Síochána and ISPs and through the means of a reporting hotline. Given that such procedures are not on a formal statutory footing and are not amenable to judicial review, there is a lack of judicial oversight. In such circumstances and in circumstances where there is very little publicly available information about the inner-workings of the soft-law mechanisms, it is difficult to identify the safeguards, if any, which are in place to ensure an adequate balance is reached between censorship and freedom of expression.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

Self-regulation by the private sector has been the traditional approach in Ireland regarding blocking and taking down Internet content. In 1998, the Report of the Working Group on Illegal and Harmful Use of the Internet recommended a system of self-regulation.[1043] recommended the establishment of a common practice code for internet service providers, as well as a hotline service.[1044] Both of these have been implemented by the Internet Service Providers Association

1040 ibid.
1041 Muwema v Facebook Ireland Ltd (No.3) [2018] IECA 104 (no. 3).
1042 ibid.
1043 Department of Justice, Equality and Reform, 'Illegal and Harmful Use of the Internet: First Report of the Working Group' (1998) 6 <http://www.justice.ie/en/JELR/IllegalUseofInternet.pdf/Files/IllegalUseofInternet.pdf> accessed 3 March 2020.
1044 ibid, 4.

of Ireland, a non-profit-company that coordinates the self-regulatory landscape.[1045]

At first it may appear ineffective as private companies cannot force each other to comply with the code of practice. However, the Department of Justice and Equality oversees both the Code of Practice and Ethics, and Hotline.ie.[1046] Additionally, Hotline.ie is sanctioned by An Garda Síochána as the national reporting mechanism in Ireland.[1047] If illegal material is traced to a server in Ireland it is reported to An Garda Síochána and 'take down' notices are issued to the service provider.[1048]

The self-regulatory scheme is qualified firstly by oversight from the Department of Justice and Equality; and secondly by the enforcement of An Garda Síochána. As Horgan points out the internet is an international medium that will require international private law to properly regulate effectively.[1049]

It may also be argued that the apparent light touch taken against liability of Internet Service Providers is further evidence of a preference for self-regulation. Section 5 of the Child Trafficking & Pornography Act 1998 made it an offence to knowingly produce, distribute, print, or publish child pornography. The 'knowingly' requirement was inserted after discussions with the working group and the Department of Justice. Internet service providers argued they could not police everything on the internet.[1050] This may seem reasonable at first, but two factors should be considered. Firstly, some larger services providers have substantial profit margins; and secondly due to evolving artificial intelligence, filtering technology does exist. Consequently, the onerous obligation argument begins to fall through. It may be questionable that a private actor that can monetise content is left to police it with minimal liability.

Although the blocking and takedown of internet content in Ireland is currently governed by self-regulation, this could very likely change very soon. At the beginning of the year a proposal for the Online Safety and Media Regulation Bill

---

1045 Law Reform Commission, *'Harmful Communications and Digital Safety Report'* (LRC 116 2016) 1.32 <https://www.lawreform.ie/news/report-on-harmful-communications-and-digital-safety.683.html> accessed 13 March 2020. (LRC 116)

1046 Internet Service Providers' Association of Ireland, 'The Voice of Online Industry in Ireland' <https://www.ispai.ie/> accessed 25 February 2020.

1047 Hotline.ie, 'Who We Are' <https://www.hotline.ie/about/> accessed 25 February 2020.

1048 ibid.

1049 'Child Pornography and the Internet—Freedom of Expression Versus Protecting the Common Good' [1999] 3 IJFL 7.

1050 Maeve McDonagh and Micheál O'Dowd, *Cyber Law in Ireland* (2015, Kluwer Law International) 372.

was published.[1051] As outlined earlier in this report, the legislation if enacted will create an Online Safety Commissioner that will ensure online services follow the guidelines set out by the proposed legislation.[1052] The Bill does not dramatically change the position, the lack of international harmonisation remains a significant obstacle to effective regulation. However, the Bill is to be welcomed for several reasons. Firstly, it would add a lot more weight to codes of practice and the sanctions would likely deter deviation from them. Secondly, it is preferable that a body established by a Statute draft the codes, instead of a non-profit company in the industry. Thirdly, it provides a legal basis for the blocking and takedown of internet content. TJ McIntyre points out how Article 10 of the European Convention on Human Rights requires measures that restrictions on freedom of expression must be 'prescribed by law.'[1053] McIntyre argues that the self-regulatory system in Ireland, where An Garda Síochána simply tells internet service providers to remove content, on the face of it breaches this provision.[1054]

In conclusion, while Ireland operates a self-regulatory scheme for the blocking and taking down of content, this involves oversight from the Department for Justice, as well as co-operation with An Garda Síochána. While the proposed new Bill will bring many improvements, issues will remain unresolved until a comprehensive international scheme is developed.

5. Does your country apply specific legislation on the 'Right to be Forgotten' or the 'Right to Delete'?

The 'Right to be Forgotten' has been a topic of concern for many academics with some feeling that the right could be utilised to rewrite history.[1055] The balance which must be struck between the 'Right to be Forgotten' and 'Freedom of Speech' is something which has also attracted major criticism from academics.[1056]

1051 Liz Dunphy, 'New bill aims to establish Online Safety Commissioner' *The Irish Examiner* (10 January 2020) <https://www.irishexaminer.com/breakingnews/ireland/new-bill-aims-to-establish-online-safety-commissioner-974746.html> accessed 27 February 2020.

1052 General Scheme of the Online Safety & Media Regulation Bill 2019. https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx accessed 12 February 2020. Media Bill 2019.

1053 TJ McIntyre, 'The curious case of internet filtering in Ireland' IT Law in Ireland (11 April 2011) <http://www.tjmcintyre.com/search/label/data%20protection> accessed 27 February 2020.

1054 ibid.

1055 Orla Lynskey 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' Modern Law Review (2015) 78(3) 533 <https://onlinelibrary.wiley.com/doi/full/10.1111/1468-2230.12126> accessed 10 February 2020.

1056 Daniel J Solove, 'The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure' Duke Law Journal (2003) 53(3) 976. <https://dx.doi.org/10.2139/ssrn.440200> accessed 12 February 2020.

On the 25 May 2018, the General Data Protection Regulation (hereinafter referred to as GDPR),[1057] came into force in Ireland, introducing a 'Right to be Forgotten' into Irish Law. Article 17 of the GDPR refers to the 'Right to Erasure', commonly known as the 'Right to be Forgotten' or the 'Right to Delete' sets out that a data subject shall have the right to request erasure of personal data concerning him or her. The Article further places an obligation on the controller of such data to comply with the request absent any undue delay where any of the grounds outlined in the Article apply.[1058] This right may be exercised where the data in question is 'inadequate, irrelevant or no longer relevant.'[1059]

While Article 17 of GDPR[1060] is now the main legislation relied upon by those who seek to avail of their 'Right to be Forgotten', prior to its introduction into Irish Law, there were other areas of law which individuals could rely upon in an attempt to have negative, private and personal information removed. Primarily, the 'Right to be Forgotten' was rooted in data protection law but it may also be seen in relation to spent convictions, defamation law and privacy law.

5.1. Data Protection Law

Prior to the coming into force of Article 17 GDPR, the Data Protection (Amendment) Act 2003 most closely represented an early form of the 'Right to be Forgotten'. Although, the 2003 Act was replaced by GDPR, section 4(2)(d)[1061] amended section 2 of the principal Act in respect of the fair processing of data to include a right to rectify data concerning an individual. While section 8 of the 2003 Act created an obligation under section 6 of the principal Act wherein the processing of data must respect the right to privacy of an individual. Furthermore, Section 8 provided that an individual could give notice in writing to a data controller, requesting that the cessation or non-commencement of the processing of any personal data regarding the applicant. However, such a request was limited to circumstances where such data processing is causing or likely to cause damage or distress to the individual or another person.

Article 17 GDPR[1062] is much broader and allows the right to be availed of where the data is no longer necessary, consent has been withdrawn for the processing, there is no overriding legitimate grounds for processing, or the data has been

[1057] General Data Protection Regulation [2016] OJ 2 127/01. (GDPR).
[1058] ibid, Article 17(1).
[1059] Case C-131/12 Google Spain and Google [2014] ECR I-000.
[1060] Article 17(1) of the GDPR.
[1061] Data Protection (Amendment) Act 2003.
[1062] General Data Protection Regulation [2016] OJ 2 127/01. (GDPR).

unlawfully processed.[1063] This was put more succinctly by the Court of Justice of the European Union in the Google Spain case as data which was 'inadequate, irrelevant or no longer relevant'.[1064]

5.2. Spent Convictions

Without the Right to be Forgotten, an ex-offender attempting to pursue a new start in life could be continuously faced with intrusion into his personal life by the media and his past. The most obvious example of this is regarding minors. Section 258 of the Children Act 2001 sets out that individuals under the age of 18, subject to some other qualifications, may not be required to disclose certain findings of guilt where such convictions are minor in nature. Similar allowances were made regarding adults under the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016. This Act establishes the circumstances under which certain convictions may be considered 'spent'.

It may be argued that the 'Right to be Forgotten' is present in section 6(2) of the 2016 Act. In accordance with this section, when asked about any previous spent convictions, other than by a court, the individual shall regard such a question as not applicable to them.[1065] Furthermore, section 6(2)(b), states that a person shall face no repercussions in failing to disclose information regarding convictions considered spent. Both the 'Right to be Forgotten' and section 6(2) of the 2016 Spent Convictions Act prevent prejudice regarding certain past convictions which are no longer relevant. Arguably, social prejudice towards those convicted of crime does not assist in rehabilitation. A minor criminal past may serve as a barricade against a meaningful re-entering into society. While both the Children Act 2001 and the Spent Convictions Act 2016 have more limitations in relation to the 'right to be forgotten' than under GDPR, they are arguably an incremental form of the 'right to be forgotten' within Irish law.

5.3. Defamation Law

It may be argued that legislation such as the Defamation Act 2009 is a form of the 'Right to be Forgotten' with provision made for the removal of certain statements under section 33.1 which prohibits further publication. The validity of this has been questioned by the Irish judiciary in Rossa v Independent Newspapers[1066] where Hamilton CJ stated that the use of defamation law by the respondent was an attempt 'to escape his past'.[1067] When questioning whether

[1063] ibid.
[1064] Case C-131/12 Google Spain and Google [2014] ECR I-000, paragraph 93.
[1065] Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 (Spent Convictions).
[1066] [1999] 4 IR 432, 470.
[1067] ibid.

defamation law acts as an early form of the 'Right to be Forgotten', one must have regard to the fact that the law of defamation can only be used where the information in question is false. If the information is true, it does not matter that it lowers the reputation of the individual in question.[1068]

The 'right to be forgotten' is a far more expansive principle than any found under defamation law. Initially, the two could be compared in that they both seek to have information removed, but the 'Right to be Forgotten' does not require that the information be false, merely that it is 'inadequate, irrelevant or no longer relevant'.[1069] To say that defamation law is an early form of the 'Right to be Forgotten' would be a hard point to argue. It is perhaps more accurate to state that they share some similarities and core elements.

5.4. Privacy Law

The 'right to be forgotten' has a clear connection with privacy law and could be argued as comprising a fundamental aspect of the right to privacy. It was established in the case of *AG v Norris,*[1070]that the scope under the constitutional right to privacy could still expand to cover more areas of personal privacy. It has been suggested that this could result in the privacy right expanding in the future and resultantly, the 'right to be forgotten' may emerge under the Constitution.[1071] The right to privacy clearly serves to protect individuals and prevent private and personal information regarding that individual being distributed. This has a clear overlap with the purpose of the 'Right to be Forgotten'. The 'Right to be Forgotten' could be strongly argued to fall within the right to privacy in that a person has both a right to their past and a right not to be held hostage by it.

A 'narrow' 'right to be forgotten' may be seen in the form of a 'Right to be delinked or delisted'. This particular right was sought in Irish law in the case of Savage v Data Protection Commissioner and Google Ireland.[1072] The plaintiff was a candidate for local election in Dublin and sought to have a thread from Reddit, labelled 'Mark Savage, North County Dublin's Homophobic Candidate' removed when his name was searched for on Google. Google claimed it was in the public interest to be aware of such information regarding public figures. The High Court emphasised the balancing exercise based on the jurisprudence of the Google Spain case,[1073] but nevertheless, it was held that Google did not carry out

---

1068 Defamation Act s 16(1).
1069 Case C-131/12 Google Spain and Google [2014] ECR I-000, para. 92 - 94.
1070 [1994] IR 36.
1071 Patrick O'Callaghan, 'The Right to be Forgotten in Ireland' (2018) in F. Werro (ed) 'The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia' (Springer, Forthcoming).
1072 [2018] IEHC 122.
1073 Case C-131/12 Google Spain and Google [2014] ECR I-000.

editing functions, i.e. they could not be required to add quotation marks etc. to the Google listings.[1074] White J, held that when looking at the Reddit discussion, and not just the URL in isolation, it would become clear upon reading that the post was an 'expression of opinion'.[1075] As a result, the plaintiff could not avail of the 'Right to be Forgotten' in this instance.[1076]

The Irish Times have published statistics regarding the number of requests made in relation to the deletion of URLs in Ireland since 29 May 2014.[1077] There had been 5,403 requests for the deletion of 17,721 URLs in Ireland alone, 35% were news stories, while 11% were social media accounts.[1078] These statistics demonstrate the high level at which the 'right to be forgotten' legislation has been utilised in Ireland. However, this also raises concerns regarding transparency as a result of potential over-deletion by data controllers attempting to prevent any summons before a data protection authority. The main and only truly on-point legislation within Ireland in relation to the 'right to be forgotten' is that of the GDPR. While strong arguments can be made in relation to other areas of law and how they perform as a limited 'right to be forgotten' prior the introduction of the 'right to be forgotten' under Article 17[1079], none offer such a comprehensive protection as is granted by GDPR.

6. How does your country regulate the liability of internet intermediaries?

Internet intermediaries, a term referring collectively to internet service providers, social network platforms or search engines,[1080] under GDPR may be obliged in several circumstances to block or take down personal data.[1081]

There is an obligation which may be placed on internet intermediaries to remove data which is defamatory and untrue to protect rights guaranteed by the

---

1074 Maureen Daly, High Court rules in the first Irish case on the 'right to be forgotten' (Beauchamps, 18 April 2018) <https://beauchamps.ie/publications/585> accessed 14 February 2020.

1075 [2018] IEHC 644.

1076 ibid.

1077 Charlie Taylor, 'Google gets 17,700 'right to be forgotten' requests from Ireland"The Irish Times (Dublin, 8 March 2018). <https://www.irishtimes.com/business/technology/google-gets-17-700-right-to-be-forgotten-requests-from-ireland-1.3418099> accessed 11 February 2020.

1078 ibid.

1079 General Data Protection Regulation [2016] OJ 2 127/01. (GDPR).

1080 Council of Europe 'Internet Intermediaries' <https://www.coe.int/en/web/freedom-expression/internet-intermediaries> accessed 15 March 2020.

1081 General Data Protection Regulation [2016] OJ 2 127/01. (GDPR).

Constitution.[1082] As set out under the Defamation Act 2009, a court may grant an order prohibiting the publication of a statement of that is defamatory[1083] and there is no defence on the part of the defendant i.e. it is a truthful statement.[1084]

The extent to which internet intermediaries are liable to remove or take-down data was explored in Muwema v Facebook Ireland Ltd.[1085] In this case, the plaintiff sought three orders against Facebook regarding an anonymous defamatory post. Firstly, an order prohibiting the publication or further publication of such posts. Secondly, an order requiring Facebook or anyone else aware of the prior order to cease and desist publishing the data in question and finally, an order requiring Facebook to identify the person(s) behind the account (which used the pseudonym TVO).

The plaintiff unsuccessfully relied upon section 33 of the Defamation Act 2009 in seeking the first two orders. Binchy J held that such orders would 'serve no useful purpose' due to the fact that the information in question was already well within the public domain and could have been posted anywhere else on the internet.[1086] The Court initially granted the third order to identify TVO by means of a 'Norwich Pharmacal' order,[1087] citing Norwich Pharmacal Co. and ors. v Commissioner of Customs and Excise[1088] as an authority for the courts 'equitable jurisdiction' to do so.[1089]

However, following the order being made, but before it had been perfected, Facebook entered new evidence in the form of an affidavit. It was argued that if TVO was identified, his life could be in danger having regard to the 'political activities' and current issues relating to human rights abuses in Uganda. As a result, Binchy J revisited his earlier decision.[1090] Upon balancing the facts of the case, it was held that TVO's right to life and bodily integrity outweighed Mr. Muwema's right to a good name. The application for a Norwich Pharmacal order identifying TVO was subsequently rescinded on the condition that as Facebook had the means to contact TVO, they were to advise that if the posts were not removed, the plaintiff was at liberty to renew his application wherein the relief sought would be granted.[1091]

1082 40.3.2 of Bunreacht Na hÉireann 1937.
1083 Defamation Act 2009 s 33(1) section 33.
1084 ibid, sction 16.
1085 Muwema v Facebook Ireland Ltd (No. 1) [2016] IEHC 519.
1086 ibid, 62.
1087 A Norwich Pharmacal order is a court granted order to disclose documents or information granted against an innocent third party which has been caught within a situation of wrongdoing.
1088 [1974] AC 133.
1089 Muwema v Facebook Ireland Ltd (No. 1) [2016] IEHC 519, 65.
1090 Muwema v Facebook Ltd (No. 2) [2017] IEHC 69 (supplemental decision).
1091 ibid, 41.

Mr. Muwema appealed this decision to the Court of Appeal,[1092] arguing that Binchy J had placed too much weight on the affidavit produced by Facebook regarding the potential mistreatment of TVO in Uganda. As a result, his right to seek damages under the Defamation Act 2009[1093] had been negatively impacted. However, the Court of Appeal stated it would not interfere in the decision of the High Court. Peart J noted that it was inevitable that the risk established should be considered to outweigh the plaintiff's right to seek damages.[1094] The Court of Appeal did confirm that under normal circumstances the plaintiff would have been entitled to a 'Norwich Pharmacal' order unmasking the identity of the anonymous poster who defamed him.[1095] This point remains good law and as a Court of Appeal decision is binding on all lower courts. In essence while internet intermediaries are not specifically liable for content, they may be made responsible to assist plaintiffs seeking to uphold their rights, specifically to reputation under the Constitution.[1096]

Issues may arise as to the extent of the internet intermediaries' obligation. In particular, the extent to which they can remove certain data from the internet in a more practical sense. One such issue is the ability to quickly disseminate data on the internet. Once data becomes 'viral', it quickly becomes increasingly difficult to remove every aspect of it from the internet. Resultantly, the obligation of the internet intermediary may be harder to fulfil. As O'Callaghan highlights, a requirement placed on the data controller to remove every aspect of the data in question, from every corner of the internet would be 'too onerous'.[1097]

However, Article 17(2) of GDPR[1098] has taken this into consideration by regulating that a data controller, having already published the data, is required to 'take reasonable steps' having regard to available technology and costs to comply with an obligation or request to remove. Article 17(2)[1099] further obligates upon the internet intermediary to inform other data controllers, in possession of the data in question, of the request of erasure. Arguably, this article also attempts to add an element of proportionality in regulating internet intermediaries while balancing a right to removal of data and the practicalities of doing so.

1092 Muwema v Facebook Ireland (No. 3) [2018] IECA 104.
1093 Defamation Act 2009, s 31.
1094 Muwema v Facebook Ireland (No. 3) [2018] IECA 104, Peart J, 39.
1095 Muwema v Facebook Ireland (No. 3) [2018] IECA 104, Peart J, 36.
1096 Article 40.3.2 of Bunreacht Na hÉireann 1937.
1097 Patrick O'Callaghan, 'The Right to be Forgotten in Ireland' (2018) in F. Werro (ed) 'The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia' (Springer, Forthcoming).
1098 General Data Protection Regulation [2016] OJ 2 127/01. (GDPR).
1099 ibid.

Currently, GDPR does not specify whether online service providers are considered data controllers in respect of user-generated data. Arguably, if they are not considered as data controllers, it raises legal uncertainty as to which of the protections and obligations under GDPR and Data Protection Acts are relevant in regulating internet intermediaries and by association, online content. Keller suggests that online service providers should comply with the 'Right to be Forgotten' rather than facing potential liability under data protection regulations.[1100] This presents a clear risk of over-removal by online service providers to prevent any decisions being made against them. This further raises issues in relation to transparency.[1101]

In its 2016 report,[1102] reference is made to the Commissioner upholding a complaint relating to a 'spent conviction'; recognising that the data in question was no longer relevant and ordered the data be removed from the search engine in line with the provisions as set out in the Spent Convictions Act.[1103] This serves as a positive example of a regulatory body enforcing the right of privacy and the right to be forgotten upon an internet intermediary or face liability.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

The current legislation in Ireland that governs content blocking and takedown, liability of internet intermediaries, and the Right to be Forgotten is not black and white. In Irish law it is a bundle of numerous laws and regulations that one must look at individually, -in order to paint a picture of how Irish laws govern internet censorship. As the topics regarding censorship have transformed over several decades, it is important to be aware of the current laws that administer such subjects. This will allow us to make an appropriate assumption as to how such laws will develop over the next five years. At present and as outlined previously, the governance of such material involves many different Irish laws and regulations, which will be outlined below.

[1100] Keller, 'The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation' (2018) 33 Berkeley Tech 326 <https://btlj.org/2018/06/volume-33-issue-1/> accessed 19 March 2020.

[1101] 2018] IEHC 122, Savage, 14.

[1102] The Annual Report of the Data Protection Commissioner of Ireland (Data Protection Commission) 2016 <https://www.dataprotection.ie/en/media/19> accessed 20 February 2020.

[1103] Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 (Spent Convictions).

This section will first look to the right that guarantees freedom of expression. This freedom is outlined in the Constitution under Article 40.6.1[1104] which states one has the right to 'freely express convictions and opinions'. It is possible to look to this Article as an example of how Ireland governs internet censorship and what people post online. A person may believe they are merely stating their opinion and exercising their freedom of expression whilst posting on the internet. However, it is also possible that their opinion could jeopardise other individuals' rights such as privacy. Due to this, for people to enjoy their right to the freedom of expression, it is important to balance it with the right to privacy.

The right to privacy is not specifically detailed in the constitution, but the courts have recognised it as an implied personal right. Kennedy & Arnold v Ireland.[1105] saw the High Court upheld the claim that telephone tapping was a breach of an unenumerated right to privacy Hamilton P stated that 'right to privacy must ensure the dignity and freedom of the individual, in the type of society envisaged by the Constitution'134. This was a clear confirmation and acknowledgement that the right to privacy is an important part of Irish legal framework.[1106] It is important to strike a balance between freedom of expression and privacy, as one without the other may lead to an Ireland where the thin line between safeguarding and surveillance may become blurred.

The progression of internet usage since its first introduction thirty years ago[1107] has certainly accelerated at a very fast pace. In 2013 82% of individuals living in Ireland had access to the internet at home, and in 2018 that figure increased to an estimated 89%.[1108] The 7% increase in a 5-year period shows how the internet has become an everyday feature in Irish homes, rivalling television and radio as a media source. The Broadcasting Authority of Ireland estimates that 52% of consumers receive their news via social media.[1109] This figure can then be used to predict that within five years usage of the internet will continue to increase.

The progression of the internet has clearly had many benefits such as social networking, contacting loved ones and E-commerce capabilities. These advancements have also led to some deceitful activity through the internet. An injunction sought by the Motion Pictures Association against Ireland's main

1104 Bunreacht Na hÉireann 1937.
1105 [1987] IR 587.
1106 '25 Years of the Internet in Ireland Marked' (*RTE*, 17 June 2016) <https://www.rte.ie/news/technology/2016/0617/796241-25-years-of-internet-in-ireland-marked/> accessed 4 February 2020.
1107 ibid.
1108 'Information Society Statistics – Households' (Central Statistics Office, 31 August 2018) <https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2018/> accessed 5 February 2020.
1109 ibid.

internet service providers saw the request to block numerous websites from which one could download films and television shows without the consent of the original producers. [1110] These websites had been alleged to have facilitated major copyright infringements, by allowing people to access certain TV Shows and Movies for free through use of these websites, generating revenue through incessant ad usage. The blocking and takedown of such websites has proven to be a positive step in internet censorship, as in some cases, the ads that were being shown on such websites, included explicit content.

Muwema v Facebook Ireland[1111] saw Facebook deal with a takedown request and identification of an anonymous user regarding defamatory information posted about the claimant. The Court declined to hold Facebook responsible for the postings of an anonymous third party to their site. Stating that the defence of innocent publication was applicable. However, then anonymous user could be identified. Subsequent to this decision, Facebook produced evidence declaring that if the person in question was to be identified, his right to bodily integrity would be at stake due to the nature of human rights abuses in Uganda at the time. The court held that 'though the plaintiff was entitled to the constitutional right to good name, the said right needed to be balanced against the right to life of another person'[1112]

As a contrast, the 2015 case of Petroceltic International plc v Aut O'Mattic[1113] saw the High Court order the defendant to remove the defamatory posts and subsequently reveal the identity of an anonymous blogger under Section 33 of the Defamation Act 2009.[1114] There is clearly a stark difference between these two cases regarding how the courts deal with the liability of internet intermediaries. Arguably the engagement of the right to life of the anonymous third party in Muwema was the factor carrying significant weight in the final decision.

The future of such cases will likely be highly discretionary and therefore judged on a case by case basis due to the liquid nature of such situations. One could be

[1110] 'Irish Film Board Telecoms the News That Members of The Motion Picture Association (MPA) Win Injunction Against Three Pirate Websites' (Screen Ireland, 5 April 2017). https://www.screenireland.ie/news/bord-scannan-na-hireann-the-irish-film-board-ifb-welcomes-the-news-that-the, Accessed 10 February 2020.

[1111] Muwema v Facebook Ireland Ltd (No. 1) [2016] IEHC 519.

[1112] Muwema v Facebook Ltd (No. 2) [2017] IEHC 69 (supplemental decision).

[1113] (HC, unreported, 20 August 2015).

[1114] LK Shields 'Norwich Pharmacal Order in Ireland: Case Law So Far (Dublin, 8 February 2016) <https://www.lkshields.ie/news-insights/publication/norwich-pharmacal-orders-in-ireland-case law-so-far> accessed 19 February 2020.

hopeful that a more solid precedent could unfold, to bring clarity to this area of the law.

As is apparent, Ireland has started to strike a clear balance between safeguarding and surveillance thus far, yet the fast-paced advancement of the internet has the capability to tip the balance.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in the online environment? If not, what needs to be done to reach such balance?

The nature of the internet allows authors of hate speech to transmit their communications easily and to a far greater audience than ever before. The biggest challenge in addressing hate speech is finding the balance between one person's right to freedom of expression, or the right of individuals to voice opinions that 'offend, shock or disturb' and the right of other individuals to not be subjected to messages of hate.[1115]

The Prohibition of Incitement to Hatred Act 1989 outlines the definition of 'hatred' in Irish law as speech against a group of persons in the State, or elsewhere, on account of race, colour, nationality, religion, ethnic or national origins, member of the travelling community or sexual orientation.[1116] It is difficult to reach a balance between freedom of expression and hate speech.. This difficulty primarily stems from the evolving and dynamic nature of content classified as hate speech. For example, some statements may be considered as humorous in some contexts but be classified as hate speech in others.[1117] Due to the development of language, slang, and translation-related issues, this can pose significant difficulties for authorities in prosecuting instances of hate speech in a consistent manner.

In the case of Karatos v Turkey it was stated that the higher the impact of speech, the more likely it is to disrupt public order.[1118] Arguably though, just because many people are offended that in itself does not prove the presence of hate speech. Irish courts have developed parameters to draw a line between speech which is merely offensive and hate speech. These rules were originally developed

[1115] *Handyside v. the United Kingdom*, (5493/72) [1976] ECHR 5 (7 December 1976), 49.
[1116] The Prohibition of Incitement to Hatred Act 1989, s1(1).
[1117] Wolfgang Benedek and Matthias C. Kettemann M, *Freedom of Expression and The Internet* (Council of Europe Publishing, 2014) 83.
[1118] *Karatos v Turkey* App No 23168/94 (ECHR, 8 July 1999).

without the reference to internet and online speech, but it was decided the same rules are applicable.[1119]

8.1. The use of legislation in preventing hate speech

Hate crime legislation plays 'a long-term role' in shaping society's evolving attitudes towards race, sexual orientation, and other minority groups. As outlined by Walters, when a society criminalises hate speech and hate crimes, it assists in changing social attitudes to reject displays of identity prejudice, creating a more positive society.[1120]

The current Irish legislation has been deemed inadequate in tackling hate crime, especially online hate crime.[1121] The Framework Decision on Racism & Xenophobia in Ireland has deemed Ireland as non-compliant. Due to wording of the legislation's definition of hatred,[1122] several groups, including disablist Hate Crime groups, were not included.[1123] A 2017 report carried out by the Irish Network Against Racism found that 57 incidents of hate speech online, between social media and newspaper websites, took place between July and December 2017.[1124] Overall, since the enactment of the 1989 Act in Ireland out of 50 prosecutions there have only been 5 convictions on hate speech.[1125] The 1989 act is inadequate in addressing separate offences in public incitement, in it does not apply to targets of individual hate and makes no reference to grounds of language.[1126]

A significant drawback of the 1989 Act is in its wording which makes successful prosecutions difficult. Section 2(1) of the Prohibition of Incitement to Hatred Act outlines that it is an offence to publish/distribute/display written material outside of a private residence that is threatening, abusive or insulting and is

---

1119 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law OJ L 328 of 6.12.2008.

1120 Walters M. '*Why the Rochdale Gang Should Have Been Sentenced As 'Hate Crime' Offenders*', (2013) 2 Criminal Law Review 131-144 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2470042> accessed 21 February 2020.

1121 Amanda Haynes and Jennifer Schweppe, *Lifecycle of a Hate Crime: Country Report for Ireland* (ICCL 2017) <https://www.iccl.ie/wp-content/uploads/2018/10/Life-Cycle-of-a-Hate-Crime-Country-Report-for-Ireland.pdf > accessed 1 February 2020.

1122 S.1 states "hatred" means hatred against a group of persons in the State or elsewhere on account of their race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation

1123 Amanda Haynes, Jennifer Schweppe and Seamus Taylor (ed), *Critical Perspectives on Hate Crime: Contributions from the Island of Ireland.* (Palgrave Macmillan, 2017).

1124 ibid.

1125 Michelle Hennessy, The Law Is Weak: Government Launches Public Consultation on Hate Speech, The Journal.ie (Ireland, 24 October 2019) <https://www.thejournal.ie/public-consultation-hate-speech-4864440-Oct2019/> accessed 2 March 2020.

1126 Amanda Haynes, Jennifer Schweppe and Seamus Taylor (ed), Critical Perspectives on Hate Crime: Contributions from the Island of Ireland. (Palgrave Macmillan, 2017).

intended or, having regard to all the circumstances, is 'likely to stir up hatred'. Effectively creating three hurdles for the prosecution to overcome. (1) Publication, (2) of threatening or abusive material, (3) that is 'likely' to 'stir up hatred'. This third hurdle is the hardest to overcome as it requires something akin to intention as an essential ingredient. This difficulty is evidenced in the so-called 'Traveller Facebook case.'[1127] In this case, the District Court heard that the accused set up a Facebook page sometime between October and November 2009. Under 'Information/description' on the page, the accused wrote that instead of using animals for shark bait they could use traveller babies instead. Likewise for feeding time at the zoo and for testing new drugs and viruses.'[1128] The accused sent the page to three of his friends and, eventually, the page had 644 members with others adding abusive material.[1129] The case was dismissed as there was reasonable doubt that there had been an intention to 'incite hatred against the Traveller community.'[1130] Other factors such as that the accused had not contributed to, or commented on the page were taken into account with the court concluding that a 'once-off insertion of material could not be deemed an incitement to hatred.'[1131] The requirement of intent means that prosecutions are difficult and contributes to the low number of convictions under this act.

8.2. What needs to be done to reach an adequate balance in Ireland?

A public consultation was launched by the Irish Government on 24 October 2019 to increase the legislation on the area of hate speech. The Minister for Justice, Charlie Flanagan and the Minister of State, David Stanton, declared that the inquiry would take place across the timeframe of 7 weeks and would include input from academics, victims of hate speech and the general public.[1132] The Law Reform Commission has recommended that the Irish Government establish a monitoring and oversight body to regulate the operation of notice and take-

---

1127 Law Reform Commission, *'Harmful Communications and Digital Safety Report'* (LRC 116 2016) 1.32 <https://www.lawreform.ie/news/report-on-harmful-communications-and-digital-safety.683.html> accessed 13 March 2020, 2.246.

1128 Siobhan Cummiskey, 'Facebooked: Anti-Social Networking and the Law' (2011) 105(9) Law Society Gazette 16, 17. <www.lawsociety.ie/globalassets/documents/gazette/gazette-pdfs/gazette-2011/november-2011.pdf> accessed 16 March 2020.

1129 ibid.

1130 Law Reform Commission, *'Harmful Communications and Digital Safety Report'* (LRC 116 2016) 1.32 <https://www.lawreform.ie/news/report-on-harmful-communications-and-digital-safety.683.html> accessed 13 March 2020, 2.246.

1131 Siobhan Cummiskey, 'Facebooked: Anti-Social Networking and the Law' (2011) 105(9) Law Society Gazette 16, 17.

1132 Michelle Hennessy, The Law Is Weak: Government Launches Public Consultation on Hate Speech, The Journal.ie (Ireland, 24 October 2019) <https://www.thejournal.ie/public-consultation-hate-speech-4864440-Oct2019/> accessed 2 March 2020.

down procedures, to act as a primary mechanism of self-regulation for social media platforms.[1133]

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

9.1. Freedom of Expression

The Irish Parliament (the 'Oireachtas') is tasked with the responsibility of configuring legislation that regulates rights, without infringing those rights disproportionately.[1134] As stated before, freedom of expression is protected in Article 40.6 of the Irish Constitution[1135] and it was given this prestigious place on the rationale of its innate part of personal dignity, autonomy.[1136] The provision also includes specific protection for public organs as educators of public opinion, namely radio, the press and cinema again as far as it does not undermine public order, morality, or the authority of the State.[1137]

9.2. Protecting other rights

The Right to Freedom of Expression cannot be viewed in a vacuum and must be viewed in consideration of other rights. There are other considerations that can come into conflict with the Right to Freedom of Expression such as public order, morality, and Constitutional rights. Such rights include (but are not limited to) privacy, autonomy, property rights and the right to earn a living.[1138] Article 40.3.1 of the Irish Constitution also has an overarching provision which overlays a duty on State to protect the personal rights of citizens, '[t]he State guarantees in its laws to respect, and, as far as practicable, by its law to defend and vindicate the personal rights of the citizen.'

The right to a good name protected by Article 40.3.2[1139] has been a major area of litigation in Ireland. As well as its place in the Constitution, it is also governed by the Defamation Act 2009. This Act was recently reviewed by the Law Reform Commission following on from a request from the Attorney General of Ireland.

1133 Law Reform Commission, *'Harmful Communications and Digital Safety Report'* (LRC 116 2016) 1.32 <https://www.lawreform.ie/news/report-on-harmful-communications-and-digital-safety.683.html> accessed 13 March 2020.

1134 Article 15.4.1 of Bunreacht Na hÉireann 1937; Heaney v Ireland [1996] 1 IR 580.

1135 Bunreacht Na hÉireann 1937.

1136 Oran Doyle, Constitutional Law: *Text, Cases and Materials* (Dublin: Clarus, 2019) 194.

1137 Article 40.6.1.(i) of Bunreacht Na hÉireann 1937.

1138 Article 40.3.1 of Bunreacht Na hÉireann 1937.

1139 Art 40.3.2 of Bunreacht Na hÉireann 1937.

The request came on foot of earlier comments by the Attorney General of the potentially chilling impact on the current level and quality of court reporting where court reporters were at risk of being sued due to minor omissions or errors.[1140] The Law Reform Commission published their findings in 2019 and recommended that privilege defences for fair and accurate reporting of proceedings should be applicable not only to professional Journalists but also to others such as bloggers, social media users and citizen journalists.[1141] This acts in favour of the balancing required between the Freedom of Expression and another right.

An inherent weakness with the Defamation Act 2009 is the need to commence legal proceedings and the associated costs. Defamation proceedings are not covered by civil legal aid, making parties liable for their own costs. The prohibitive expense involved with an action of this nature may deter the less affluent seeking to restore their good name, with the Act arguably only assisting those who can afford its protection.[1142] As a result creates an imbalance between freedom of expression and protection of a good name by creating a financial constraint.

If we look to the case of Mahon v Keenawe can see the Irish courts engage in a discussion on freedom of expression and the question of whether a tribunal has the power to order journalists to reveal their sources, and the test to be applied in such circumstances.[1143] As stated by Justice Fennelly in the case, 'where, as in this case, fundamental rights are invoked as a restraint on the exercise of statutory powers, the courts are increasingly called upon to strike a balance'.[1144] Further in the judgment after discussion of the European Convention on Human Rights jurisprudence the court declared, 'these judgements emphasise not merely the fundamental right to freedom of expression but, in the case of the press, its indispensable contribution to the functioning of a democratic society.'[1145]

An aspect of privacy explored in the courts is the distinction as to whether the invasion of privacy is deliberate, conscious and unjustified as seen in Kennedy & Arnold v Ireland[1146] and more recently in K (L) (A Minor) v Independent Star

1140 Law Reform Commission, Privilege for Reports of Court proceedings under the Defamation Act 2009(LRC 121-2019) at 7.
1141 ibid, at 63.
1142 Sarah Frazier, 'Liberty of Expression in Ireland and the Need for a Constitutional Law of Defamation' (1999) 32 Vanderbilt Journal of Transnational Law 391.
1143 [2009] 2 ILRM 373.
1144 ibid, at para 23.
1145 ibid.
1146 [1987] IR 587.

and Ors.[1147] The High Court case of Hickey & Agnew (a minor) v Sunday Newspapers Ltd shows the importance of this distinction with Kearns J stating that to hold otherwise 'would represent a radical ratcheting up of the right to privacy at the expense of the right of freedom of expression to a degree which, in my view, should more properly be the subject matter of legislation.'[1148] In Hickey & Agnew (a minor) v Sunday Newspaper Ltd there is an issue that comes to light when we see publications, who do not necessarily qualify as having published a defamatory statement, but their behaviour is still considered reprehensible. Kearns J in his judgment stated that 'the exercise in which the defendant newspaper engaged in respect of these two publications represented the lowest standards of journalism imaginable. It is a regrettable fact of life that such material sells newspapers.'[1149]

9.3. Are these rights balanced?

From the research, there does not appear to be sufficient balancing of some of the different rights involved. The differing and evolving view of what people consider a breach of rights has complicated the area. For example, illustrating where freedom of expression online and other rights come into competition, in copyright law the traditional view is the creator, i.e. author, producer, singer, have proprietary rights to such material. To take and use without permission is a breach of copyright laws. Arguably, in some respects, as per Article 40.3[1150] it may also be a breach of a person's right to earn a living and their right to own property and now a breach of intellectual property rights.[1151] The other side of the argument is that the internet is an open forum and when content is uploaded it is no longer your property per se.[1152]

The case of Open Door and Well Woman v Ireland[1153] the Court of Human Rights shows how the Court balances rights and apparent breaches of same. The Court specifically looked at how Ireland had balanced the right to freedom of expression in light of Article 2, 17 and 60 of the ECHR. In this case there had been a perpetual injunction granted against the supply of information on abortions to pregnant women.[1154] The question the Court asked was 'whether or not it was justified under Article 10(2) ECHR by reason of being a restriction

[1147] [2010] IEHC 500.
[1148] [2010] IEHC 349, para 66.
[1149] ibid.
[1150] Art 40.3 of Bunreacht Na hÉireann 1937.
[1151] Irish Trade Marks Act 1996; The Patents Act 1992; The Copyright and Related Rights Act 2000.
[1152] Gibson, Anna, 'Safe Spaces and Free Speech: Effects of Moderation Policy on Structures of Online Forum Discussions.' [2017] <https://doi.org/10.24251%2Fhicss.2017.284> accessed 27 February 2020.
[1153] Open Door and Dublin Well Woman v Ireland [1992] 14 EHRR 131
[1154] ibid, at 53.

'prescribed by law', which was necessary, in a democratic society on one or other of the grounds specified in the Article 10(2)'.[1155] It was found that 'that the restraint imposed was disproportionate to the aims pursued',[1156] and that Ireland had breached Article 10 of the ECHR.

9.4. If not, what needs to be done?

For Ireland, an investment of resources into the area is recommended. For example, creating a parameter for jurisdiction intention, what rights are incorporated and a clear definition of property.[1157] It is suggested that clear guidelines should be given to police to allow them to investigate complaints and not place the onus on the ISP or the social media group to take down information.[1158]

It was recognised in Sony Music & Ors v UPC, that a generalised response from the legislature may be needed to cover the entirety of such issues, but that if the Court can deal with the issue at hand then that is what they will do.[1159] The proposed Online Safety and Media Regulation Bill has potential to break new ground,[1160] especially as it would place the onus on the newly established Commissioner to regulate online content, proactively ensuring that there is a sufficient balance is achieved.

10. How do you rank the access to freedom of expression online in your country?

10.1. Ranking

After intensive research into the freedom of expression online in Ireland, we would rank Ireland 3 out of 5. Ultimately, viewing the situation overall, freedom of expression and right to information prevails over certain forms of censorship. This ranking is due to several factors, which I will outline below.

1155 ibid, at 55.

1156 ibid, at 80.

1157 Hannibal Travis, Cyberspace Law (Routledge, Taylor & Francis Group 2013).

1158 Eva Nagle, 'To Every Cow Its Calf, to Every Book Its Copy: Copyright and Illegal Downloading after EMI (Ireland) Ltd and Ors v Eircom Ltd [2010] IEHC 108' (2010) 24 Int'l Rev L Computers & Tech 309.

1159 Sony Music Entertainment (Irl) Ltd and Others v UPC Communications Irl Ltd (No 1) [2015] IEHC 317.

1160 General Scheme of the Online Safety & Media Regulation Bill 2019. https://www.dccae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx accessed 12 February 2020.

10.2. Factors which influence ranking

Article 40.6.1.(i) of the Irish Constitution states that one has the right to freely express convictions and opinions. However, an assertion is made, to limit this freedom, by stating that media may not be used to undermine public order, the morality, or authority of the State. This 'limitation' is restrictive, yet necessary. The most positive aspect to this concept comes from an understanding of the impact the media can have on individuals.[1161] The effect of the media on individuals has increased drastically over the years, becoming more and more influential.[1162] Should the mainstream media contain unlawfully biased, damaging or unpleasant content, one might be wrongfully influenced.

Another criticism of the freedom of expression lies in its balance with privacy. Privacy is outlined in Kennedy v Ireland[1163] where Hamilton J held that the right to privacy was one of the unenumerated rights recognised by Article 40.3 of the Constitution. In some cases, the right to a good name trumps the right to freedom of expression, meaning sometimes, where one may freely express their opinions about an individual, they could be penalised for damaging that individual's name.

Media and reporters have the freedom to present Ireland's citizens with information subject to some limitations. The information provided must be for an educational purpose and must not undermine the State or public morality.[1164] Censorship to prevent file sharing is minimally intrusive into our right to information, especially when contrasted with other countries such as Algeria who blocked access to the internet for all when State exams where leaked online to prevent cheating by students[1165] There is a clear need for reform for example where ISPs are being called upon to renew blocking and filtering. The ISP Association of Ireland in a press statement argued that it is not the responsibility or obligation of an ISP to do this.[1166] Following the enactment of the Irish Constitution, censorship became a huge issue.[1167] Previously, any information not in accordance with the beliefs of the Catholic Church was 'censored'. Censorship in Ireland has evolved to reflect the importance of individual rights and freedom to information. While Ireland has dealt very well with censorship

---

1161 Valkenburg, Peter, & Walther (2016) 'Media Effects: Theory and Research' Annual Review of Psychology. 67: 315–338.

1162 ibid.

1163 [1987] IR 587.

1164 Article 40.6.1 of Bunreacht Na hÉireann 1937.

1165 Nour Youssef, 'Algeria's Answer to Cheating on School Exams: Turn off the Internet' New York Times (New York, 21 June 2018).

1166 ISP Association Responds to Porn Filtering Debacle, Michael Neuton, Technology.ie, 26 July 2013.

1167 Joan Fitzpatrick Dean, Riot and Great Anger: Stage Censorship in Twentieth Century Ireland (University of Wisconsin Press 2004).

in relation to freedom of information, with the ever-developing technology of today's world, further development is required. TJ McIntyre argues that the self-regulatory system in Ireland, where An Garda Síochána may request internet service providers to take down content absent a court order or any judicial oversight or legislative authority, could be in breach of Article 10 of the ECHR.[1168]

10.3. Concluding remarks

The ranking for Ireland would be higher if a body were established under legislation with the authority to request removal of content when specific conditions were met. For example, the Irish Human Rights and Equality Commission in December 2019 in its Review of the Prohibition of Incitement to Hatred Act 1989 recommends that the State establish an alternative reporting mechanism of hate crimes.[1169]

11. How do you overall assess the legal situation in your country regarding internet censorship?

In Ireland, the legal situation is evolving albeit slowly. Ireland has a history of reacting in an ad hoc fashion or to mould previous precedents to fit the new issues.[1170] As a common law system, it has its advantages as the judiciary are enabled (to some degree) to react on the ground. That however only happens with judges who have an interest and are up to date with technology and international jurisprudence.[1171] Most legislation regarding internet censorship comes from the EU or is enacted to conform with our international obligations under various conventions i.e. Istanbul Convention.

The onus is usually placed upon an affected individual to seek removal or rectification of offensive or incorrect information online. The individual will usually have to report the issue to the hosting site and is reliant upon the individual site's procedures. If these individual mechanisms fail the next step normally involves litigation of some kind, with the risk of substantial associated legal costs.

1168 TJ McIntyre, 'The curious case of internet filtering in Ireland' IT Law in Ireland (11 April 2011) <http://www.tjmcintyre.com/search/label/data%20protection> accessed 27 February 2020.

1169 Amanda Haynes, Jennifer Schweppe and Seamus Taylor (ed), Critical Perspectives on Hate Crime: Contributions from the Island of Ireland. (Palgrave Macmillan, 2017).

1170 Eva Nagle, 'To Every Cow Its Calf, to Every Book Its Copy: Copyright and Illegal Downloading after EMI (Ireland) Ltd and Ors v Eircom Ltd [2010] IEHC 108' (2010) 24 Int'l Rev L Computers & Tech 309.

1171 ibid.

The Irish law regarding censorship is not black and white and often struggles, it seems, to keep step with the ever-expanding concept of the internet, alongside all the legal implications which that entails. Akin to the Irish Constitution are the right to privacy and freedom of expression under Articles 10 and 8 of the ECHR. Data protection law plays a vital role when it comes to the acquisition of new 'smart' technologies, such as smart speakers, smart doorbells and smart watches. Arguably, it is vital that the law covers the aspect entailing the right to privacy that people are entitled to enjoy, whilst also maintaining the balance between censorship and surveillance.

Judges have been willing to expand the law as much as possible when someone's intellectual property rights (and by the same token their finances) are affected.[1172] One may argue that there is scope for further expansive interpretation in other areas of law, if the rights that are affected by online activity outweigh the right to freedom of expression. However existing legislation may only stretch so far. Therefore, specific legislative provisions dealing with online content and its policing are required.

[1172] Copyright and Related Rights Act 2000, s 127.

Conclusion

To conclude, under Irish law, freedom of expression has a constitutional status, but it is carefully balanced with other substantial rights such as the right to privacy and the right to a good reputation. Ireland has enacted laws to address several concerns including censorship of publication, defamation, ensuring adequate measures of data protection, and protecting the freedom of information. It is only recently that online safety has become a matter garnering the attention of the Government in respect of policy reform to ensure online safety. Ireland does not have a definition for online censorship, instead Ireland uses language such as 'protection', 'safety', 'privacy' and 'online safety' when referring to harmful online activities. The new Online Safety and Media Regulation Bill 2019 is Ireland's attempt at tackling the online safety issues. It is still at Bill stages and has not yet been enacted into law.

The right to be forgotten under Irish Law is governed by the Data Protection (GDPR) Act 2018, enacted in response the EU GDPR Regulations. However, core elements and policies underlying the right to be forgotten can be seen in Irish law prior to the GDPR's enactment. Most notably the legislation regarding spent convictions served as an early form of the right to be forgotten. Nevertheless, no area offered such thorough protection, as is granted under the Data Protection Act 2018 GDPR. The precise scope of the liability afforded to internet intermediaries cannot be easily qualified. The liability attributable to an internet intermediary in court proceedings will broadly depend on the facts of individual cases This obligation is not limited to the takedown of data but is an expansive obligation which can extend to identification of anonymous users of internet intermediaries. Furthermore, such obligations may be removed or amplified, not because of the internet intermediaries' actions necessarily. Notwithstanding, due to the multitude of surrounding factors it is quite difficult to predict the extent of obligations placed upon these intermediaries.

Hate Speech and its regulation in Ireland is currently at a very fragile state, with the Prohibition of Incitement to Hatred Act 1989 being the most up to date legislation in this area. However, the Government has recognised the need for change following the Human Rights and Equality Commission's Report on Hate Speech in Ireland. In ranking Ireland, this group recognises that there is a need for more protection Online.

Table of legislation

Provision in Irish language	Corresponding translation in English
Bunreacht Na hÉireann	The Constitution of Ireland

Bibliography

English titles

Legislation

Broadcasting Act 2009.

Broadcasting (Amendment Act) 2007.

Censorship of Films Act 1923.

Censorship of Publications Act 1929.

Censorship of Publications Act 1946.

Children Act 2016.

Child Trafficking and Pornography Act 1998.

Civil Legal Aid Act 1995.

Criminal Law Amendment Act 1935.

Criminal Justice (Legal Aid) Act 1962.

Criminal Justice (Spent Convictions) Act 2001.

Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 (Spent Convictions).

Criminal Justice (Victims of Crime) Act 2017.

Copyright and Related Rights Act 2000.

Data Protection Act 2018.

Data Protection (Amendment) Act 2003.

Data Protection Act 1988.

Defamation Act 2009.

Directive 2000/31/EC of the European Parliament and of the Council 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on Electronic Commerce'), [2000], OJ L 178/1.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, [2001], OJ L 167/10.

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, [2004], OJ L 157/45, corrected version in [2004], OJ L 195/16.

European Convention on Human Rights Act 2003.

Equal Status Acts 2000-2018.

Equality Act 2004.

European Convention on Human Rights 1950.

Freedom of Information Act 2014.

International Covenant on Civil and Political Rights 1966.

Online safety and Media Regulation Bill 2019.

Prohibition of Incitement to Hatred Act 1989.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The Patents Act 1992.

Trade Marks Act 1996.

United Nations General Assembly Resolution 2200A (XXI) 16 December 1966, in force from 23 March 1976.

Reports

Benedek W, and Kettemann M, Freedom of Expression and The Internet (Conseil de l'Europe 2014).

Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law OJ L 328 of 6.12.2008.

Department for Communications, Climate Action & Environment, 'The Action Plan for Online Safety 2018-2019' (The Government of Ireland 2019). (action Plan).

Department of Justice, Equality and Reform, 'Illegal and Harmful Use of the Internet: First Report of the Working Group' (1998).

Law Reform Commission, 'Harmful Communications and Digital Safety Report' (2016).

Law Reform Commission, 'Privilege for Reports of Court Proceedings Under the Defamation Act 2009' (LRC 121 2019).

Law Reform Commission, Report on Privity of Contract and Third-Party Rights (LRC 88-2008).

General Scheme of the Online Safety & Media Regulation Bill 2019 - Amending the Broadcasting Act 2009.

Daly M, 'High Court rules in the first Irish case on the 'right to be forgotten' (Beauchamps, 18 April 2018).

Schweppe J, 'Online Hate Speech (And Hate Crime Online)' (University of Limerick, 2017).

The Annual Report of the Data Protection Commissioner of Ireland (Data Protection Commission) 2016.

The National Advisory Council for Online Safety (Department for Communications, Climate Action & Environment.

The National Advisory Council for Online Safety Progress (Report, February 2019).

Books

Craig P. and De Burca G., EU Law: Texts, Cases and Materials (6th edn, Oxford University Press 2015).

Doyle O., Constitutional Law: Text, Cases and Materials (Dublin: Clarus Press, 2019).

Fitzpatrick Dean J., Riot and Great Anger (University of Wisconsin Press 2010).

Hedley S., The Law of Electronic Commerce and The Internet In The UK And Ireland (Cavendish 2006).

McDonagh M., and O'Dowd M., Cyber Law in Ireland (2015, Kluwer Law International)

O'Callaghan P, 'The Right to be Forgotten in Ireland' (2018) in F. Werro (ed) 'The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia' (Springer, Forthcoming)

Schweppe J. and Taylor S., Critical Perspectives on Hate Crime: Contributions from the Island of Ireland (Palgrave Macmillan 2017).

Travis H., Cyberspace Law (Routledge, Taylor & Francis Group 2013).

Periodicals

Dunphy L., 'New bill aims to establish Online Safety Commissioner' The Irish Examiner (10 January 2020)
< https://www.irishexaminer.com/breakingnews/ireland/new-bill-aims-to-establish-online-safety-commissioner-974746.html> accessed 27 February 2020.

Frazier F., 'Liberty of Expression in Ireland and the Need for a

Cummiskey S, 'Facebooked: Anti-Social Networking and the Law' (2011) 105(9) Law Society Gazette 16.

Constitutional Law of Defamation' (1999) 32 Vand J. Transnational Law 391.

General Scheme of the Online Safety & Media Regulation Bill 2019.

Hennessy M, 'The Law Is Weak': Government Launches Public Consultation on Hate Speech' Journal.ie (2019).

Horgan R., 'Child Pornography and the Internet—Freedom of Expression Versus Protecting the Common Good' (1999) 3 IJFL 7.

Keller D., 'The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation' (2018) 33(1) Berkeley Tech 326.

Kennedy R.., 'No three strikes for Ireland (yet): Copyright Law and individual liability in recent internet file sharing litigation' (2011) 14(1) Journal of Internet Law 15

Kenny D., and Conor C., 'A One Person Supreme Court? The Attorney General, Constitutional Advice to Government, and the Case for Transparency (1 April 2019). Dublin University Law Journal (2019, Forthcoming).

Lynskey O., 'Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez' (2015) 78(3) Modern Law Review 533.

Nagle E., 'To Every Cow Its Calf, to Every Book Its Copy: Copyright and Illegal Downloading after EMI (Ireland) Ltd and Ors v Eircom Ltd [2010] IEHC 108' (2010) 24 Int'l Rev L Computers & Tech 309.

Solove D.J., 'The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure' Duke Law Journal (2003) 53(3) Duke Law Journal 976.

Sychold M., 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' (Swiss Institute of Comparative Law, Lausanne, 2016).

Taylor C., 'Google gets 17,700 'right to be forgotten' requests from Ireland' The Irish Times (Dublin, 8 March 2018).

Valkenburg P.M., Peter J., and Walther J.B., 'Media Effects: Theory and Research' (2016) 67 Annual Review of Psychology 315

Walters M. 'Why the Rochdale Gang Should Have Been Sentenced As 'Hate Crime' Offenders',' (2013) 2 Criminal Law Review.

Werro F., 'The Right to Inform v The Right to be Forgotten: A Transatlantic Clash' (2009) 'Liability in the Third Millennium' Georgetown Public Law Research Paper No.26.

Youssef N., 'Algeria's Answer to Cheating on School Exams: Turn off the Internet' New York Times (New York, 21 June 2018).

Zagaris B., and Psilakis A., 'Extradition' (2019) 35 IELR 134.

Digital resources

'25 Years of the Internet in Ireland Marked' (RTE, 17 June 2016) https://www.rte.ie/news/technology/2016/0617/796241-25-years-of-internet-in-ireland-marked/ accessed 4 February 2020.

'Information Society Statistics – Households' (Central Statistics Office, 31 August 2018) https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2018/ accessed 5 February 2020.

'Irish Film Board Telecoms the News That Members of The Motion Picture Association (MPA) Win Injunction Against Three Pirate Websites' (Screen Ireland, 5 April 2017) https://www.screenireland.ie/news/bord-scannan-na-hireann-the-irish-film-board-ifb-welcomes-the-news-that-the , Accessed 10 February 2020.

'Over 50% of Irish people expected to own a smart speaker by 2023' (Irish Times, 25 April 2019) https://www.irishtimes.com/business/technology/over-50-of-irish-people-expected-to-own-a-smart-speaker-by-2023-1.3869382
Accessed 5 February 2020.

< https://www.dataprotection.ie/en/media/19> accessed 20 February 2020.

<https://www.irishtimes.com/news/ireland/irish-news/irish-man-pleads-guilty-to-child-abuse-image-offences-in-us-court-1.4165075> accessed 21 February 2020.

2016 Annual Report of the Data Protection Commissioner of Ireland' (Data Protection Commission) < https://www.dataprotection.ie/en/media/19> accessed 20 February 2020.

An Garda Síochána, 'An Garda Síochána Sign MOU with UPC on the Restriction of Child Sexual Abuse Material Online' <https://www.garda.ie/en/About-Us/Our-Departments/Office-of-Corporate-Communications/Press-Releases/2014/November/An-Garda-Siochana-Sign-MOU-with-UPC-on-the-Restriction-of-Child-Sexual-Abuse-Material-Online.html> accessed 25 February 2020.

Beauchamps, 'Beauchamps' involved in a Commercial Court case which blocks illegal live streaming' <https://beauchamps.ie/publications/747> accessed 25 February 2020.

Taylor C, 'Google gets 17,700 'right to be forgotten' requests from Ireland' The Irish Times (Dublin, 8 March 2018).

Gibson A, 'Safe Spaces and Free Speech: Effects of Moderation Policy on Structures of Online Forum Discussions.' [2017] < https://doi.org/10.24251%2Fhicss.2017.284> accessed 27 February 2020.

Hotline.ie, 'Types of Online Content That Should be Reported'
<https://www.hotline.ie/contact-us/what-you-can-report/>
accessed 25 February 2020.

Hotline.ie, 'Who We Are' <https://www.hotline.ie/about/> accessed 25 February 2020.

http://www.irishstatutebook.ie/eli/1989/act/19/enacted/en/html.

http://www.irishstatutebook.ie/eli/1994/act/2/enacted/en/html.

http://www.irishstatutebook.ie/eli/1997/act/26/enacted/en/html.

http://www.irishstatutebook.ie/eli/2017/act/28/enacted/en/html.

http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print#sec60.

http://www.irishstatutebook.ie/eli/cons/en/html.

https://www.dccae.gov.ie/en-ie/communications/legislation/Documents/154/General_Scheme_Online_Safety_Media_Regulation_Bill.pdf.

https://www.echr.coe.int/Documents/Convention_ENG.pdf.

https://www.echr.coe.int/Documents/Convention_ENG.pdf.

https://www.irishtimes.com/news/crime-and-law/courts/high-court/data-commissioner-google-win-appeal-over-right-to-be-forgotten-1.3395053.

https://www.oireachtas.ie/en/bills/bill/2017/63/.

Internet Service Providers' Association of Ireland, 'Code of Practice and Ethics', 10 <https://www.ispai.ie/wp-content/uploads/2013/09/Code-of-Practice-and-Ethics.pdf> accessed 25 February 2020.

Internet Service Providers' Association of Ireland, 'The Voice of Online Industry in Ireland' <https://www.ispai.ie/> accessed 25 February 2020.

ISP Association Responds to Porn Filtering Debacle, Michael Neuton, Technology.ie, 26 July 2013.

LK Shields 'Norwich Pharmacal Order in Ireland: Case Law So Far (Dublin, 8 February 2016)
< https://www.lkshields.ie/news-insights/publication/norwich-pharmacal-orders-in-ireland-case law-so-far> accessed 19 February 2020.

PwC, '7 things you need to know about the proposed Online Safety and Media Regulation Bill' (PwC, 29 January 2020)
<https://www.pwc.ie/services/consulting/insights/7-things-to-know-about-online-safety-media-regulation-bill.html>accessed 20 May 2020.

Review of The Prohibition of Incitement to Hatred Act 1989 (Irish Human Rights and Equality Commission submission to the Department of Justice and Equality public consultation 2019) <https://www.ihrec.ie/app/uploads/2019/12/Review-of-the-Prohibition-of-Incitement-to-Hatred-Act-1989.pdf> accessed 18 February 2020.

'Rights of Individuals' under the General Data Protection Regulation' (Data Protection Commission).
<https://www.dataprotection.ie/en/individuals> accessed 20 February 2020.

Bowers S., 'Almost 2,000 child abuse websites to be blocked under new initiative: Internet users will be redirected to a Garda 'stop' page when trying to view illicit material' Irish Times (Dublin 10 February 2020)
<https://www.irishtimes.com/news/crime-and-law/almost-2-000-child-abuse-websites-to-be-blocked-under-new-initiative-1.4168830> accessed 25 February 2020.

The Annual Report of the Data Protection Commissioner of Ireland (Data Protection Commission) 2016.

McIntyre TJ., 'The curious case of internet filtering in Ireland' IT Law in Ireland (11 April 2011)
< http://www.tjmcintyre.com/search/label/data%20protection>
accessed 27 February 2020.

Case law

AG v Norris [1994] IR 36.

Case C-131/12 Google Spain and Google [2014] ECR I-000

C-18/18 - Glawischnig-Piesczek [2019] ECR I-773.

CG v Facebook Ireland ltd. and McCloskey [2015] NIQB 28.

Cornec v Morrice and others [2012] 1 IR 807.

EMI Records (Ireland) Limited et al. v Eircom Limited and BT Communications Ireland Limited [2005] 4 Irish Reports 148,

EMI Records v UPC Communications Ireland Ltd [2010] IEHC 377, [2010] ECDR 17.

Erbakan v Turkey App No 59405/00 (ECHR ,6 July 2006).

Gilchrist & Rogers v Sunday Newspapers Ltd [2016] IECA 296

Handyside v The United Kingdom App No 5493/72. (ECHR, December 1976)

Heaney v Ireland [1996] 1 IR 580.

Hickey and Agnew (A Minor) v Sunday Newspapers Ltd [2010] IEHC 349.

Irish Times Ltd v Ireland [1998] 1 IR 359, 405.

K (A Minor) v Independent Star [2010] IEHC 500.

Karatos v Turkey App No 23168/94 (ECHR, 8 July 1999).

Kennedy and Arnold v Attorney General [1987] IR 587.

Mahon v Keena [2009] 2 ILRM 373.

McGee v Attorney General [1974] IR 284.

Muwema v Facebook Ireland Ltd [2016] IEHC 519 (no. 1).

Muwema v Facebook Ireland Ltd [2017] IEHC 69 (no. 2).

Muwema v Facebook Ireland Ltd [2018] IECA 104 (no. 3).

Norwich Pharmacal Co. and Ors. v Commissioner of Customs and Excise [1974] AC 133.

Oblique Financial Services Ltd v Promise Production Company [1994] 1 ILRM 74, 3.

Open Door and Well Woman v Ireland [1992] 14 EHRR 131.

Petroceltic International Plc v Aut O'Mattic A8C Ireland Ltd (HC, unreported, 20 August 2015).

Rossa v Independent Newspapers [1999] 4 IR 432, 470.

Ryan v Attorney General [1965] IR 294 (SC) 312 – 313.

RyanAir v Unister [2013] IESC 14.

Savage v Data Protection Commissioner and Google Ireland [2018] IEHC 122.

Sony Music Entertainment (Ireland) Ltd & Ors v UPC Communications Ireland Ltd [2016] IECA 231.

Sony Music Entertainment (Irl) Ltd and Others v UPC Communications Irl Ltd (No 1) [2015] IEHC 317.

The Football Association Premier League Ltd v Eircom Ltd t/a Eir & Ors [2019] IEHC 615.

United States v Eric Eoin Margues, US. District Court for the District of Maryland, Case No. 13-1789 JKS.

Irish titles

Legislation

Bunreacht Na hÉireann, 1937.

ELSA Italy

Contributors

National Coordinator

Andreina Bove

National Researchers

Raffaella Di Sario

Carla Conforti

Lucia Rosaria Muro

Pierfrancesco De Felice

Federica Paolucci

Martina Caslini

Valeria Argento

Eugenio Ciliberti

Anna Zilio

Daniele Fabris

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

'Anyone has the right to freely express their thoughts in speech, writing, or any other form of communication'.[1173] So reads the Article 21, subsection 1 of the Italian Constitution: freedom of expression stands up as a constitutionally guaranteed right. Freedom of expression has been defined by the Constitutional Italian jurisprudence as the 'milestone of the democratic order', as 'condition of the way of being and life development of the Country in all its cultural, political and social aspects'.[1174] Starting from this premise, the Constitutional Court develops two notable consequences. The first one leads to refer to the Article 21 of the Constitution not just the protection of the 'Right to Inform' as an active profile of the freedom of expression, referring to those who operate in the media system, but also the protection of the 'right to information' as a passive profile referred to all the citizens as components of 'that public opinion' on which democracy is based.

Moving in this direction, we go straight to the second consequence. The recognition of a 'right to information', connected to the freedom of expression, leads the Court to design a values juxtaposition of the rights guaranteed in the Article 21: 'individual' and 'functional'.[1175] Every functional conception of the freedom of expression advances or justifies intimately contradictory claims: it constantly demands and justifies absolute freedom and equally absolute limits of the invoked freedom, both from a subjective and objective point of view.[1176]

In its subsections the Article 21 focuses on a series of provisions specifically dedicated to the press, according to which is imposed the prohibition of preventive checks and, moreover, the possibility of seizure in the crime events expressly indicated by the law.

At last but not least, the Article 21 sets towards all the manifestations of thought, a general limit identified in the respect of 'morality'. In a parallel view to this explicit limit, the Constitutional jurisprudence, in numerous rulings, brings out the presence of a series of implicit limits connected to the protection of values of Constitutional relevance in a prospective of conflict with freedom of expression. These are values concerning the honour, the reputation and the

[1173] Article 21 Costituzione della Repubblica Italiana.
[1174] Corte Costituzionale della Repubblica Italiana, Sent. N. 84/1969.
[1175] "La giurisprudenza della Corte Costituzionale Italiana in tema di media" – Enzo Cheli, 6 giugno 2013.
[1176] "La libertà di manifestazione del pensiero nell'ordinamento italiano" – Carlo esposito - Rivista Italiana Per Le Scienze Giuridiche (Francesco Schupfer, Guido Fusinato).

discretion of the person; public order; State security; the proper conduct of justice; the protection of some forms of secrecy. These implicit limits, in the Court's view, can condition, but they cannot in any way denaturalise or cancel freedom of expression. From this assertion rise the need for a stable balance, case by case, between freedom of expression and other fundamental rights always in respect of the principles of the reserve of law and of the reserve of jurisdiction, principles which, in a Constitutional structure, represent the strongest instruments to build a protection of fundamental freedoms.[1177]

In order to fully understand the pigmented *ratio* underlined by the Article 21, we must consider a specific focus: the limits of the so-called 'Right to Chronicle' to get the 'stable balance' we are looking for.

Both the Italian legal literature and the case law have constantly affirmed that the exercise of the 'Right to news reporting' (*diritto di cronaca*) and of the freedom of the press guaranteed in the Article 21 of the Constitution represents a cause of justification within the meaning of the Article 51 of the Criminal Code, thus making the acts (the communication of information damaging the honour, the dignity or the reputation of another person) non punishable. A landmark judgment of the Court of Cassation (*Cassazione civile*, sez. I, 18 October 1984), constantly applied by Civil and Criminal courts, has set out the three criteria for the application of the Article 51:

- The social utility or social relevance of the information;
- The truthfulness of the information (which may be presumed (*verità putativa*) if the journalist has seriously verified his or her sources of information);
- Restraint (*continenza*), referring to the civilised form of expression, which must not 'violate the minimum dignity to which any human being is entitled'.[1178]

Starting from the explanation of these criteria and looking at today's and future needs, it can be certainly established that the experience of the past leads to a positive judgment on the adaptability of the Constitutional framework relating to freedom of expression (especially of the media system): a framework that has been able to absorb the pushes of a technological evolution through the evolutionary interpretations adopted in the Constitutional justice.[1179]

[1177] "La giurisprudenza della Corte Costituzionale Italiana in tema di media" – Enzo Cheli, 6 giugno 2013.
[1178] "Italy's remarks on freedom of opinion and expression and the situation of journalists" - Ministry of Foreign Affairs Inter-ministerial Committee for Human Rights.
[1179] "La giurisprudenza della Corte Costituzionale Italiana in tema di media" – Enzo Cheli, 6 giugno 2013.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

In relation to technological progress and the birth of new mass media, it was necessary to create a discipline that could handle problematic situations created online. This refers to the publication of illegal content on a large scale, such as those related to the dissemination of child pornography, contents that incite to hatred or for the purpose of terrorism, and to the violation of copyrights. The Italian legislator implemented European Directive 2000/31/EC with Legislative Decree 70/2003, providing for three categories of digital intermediaries ('mere conduit' activities, which is a mere transport activity; caching activities, which are temporary storage service providers; hosting activities, which are service providers that permanently store the information provided by users) which, depending on the level of their involvement in the user's activities, enjoy different liability exemption regimes. Article 15 of the above legislative decree provides, in the first paragraph, that 'in the provision of an information society service, consisting in the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, provided that that service provider: (a) has no actual knowledge that the activity or information is unlawful and, as regards actions for damages, is not aware of facts or circumstances which would make it apparent that the activity or information is unlawful; (b) as soon as it becomes aware of such facts, it shall, on notification from the competent authorities, take immediate action to remove the information or to disable access to it.' In addition, the competent judicial or administrative authority may request, even as a matter of urgency, that the internet service provider prevent or put an end to the violations committed, so that the effects of the crime cease and fewer people are reached.

To all types of internet service provider, the administrative and judicial authorities can not only ask to delete certain contents, but also to disclose the identity of those who have used the service in order to be able to implement the related sanctions, otherwise, if they decide not to collaborate, would respond civilly of their actions or omissions. This rule should not be interpreted as if they were exempt from having to carry out a supervisory activity: this would entail a huge activity of the internet service provider which would end up burdening its economy and work in general. At the same time, it is stated in the regulatory provision that if the internet service provider becomes aware of illegal content on its platform, it is obliged to inform the administrative and judicial authorities. Surely, this argument only applies if the publication of the content is completely out of control; if the internet service provider, on the basis of its own business

decision, decides to control each publication by creating a filter system, it would be responsible for the illegal content on its platform.[1180]

Judgment No. 7708 of 2019 of the Court of Cassation clarified some important issues by taking the opportunity of an appeal by Reti Televisive Italiane S.p.a. against the Yahoo search engine.[1181] In the decision of the Court of Cassation[1182] we read the definition of hosting provider, i.e. the provider of information society services who carries out an activity that goes beyond a purely technical, automatic and passive service, and instead engages in active conduct, competing with others in the commission of the offence, in order to remain exempt from the general regime of exemption under Legislative Decree no. 70 of 2003, Article 16, since his civil liability must act according to the common rules.[1183] In the context of information society services, the responsibility of the hosting provider remains with the service provider who has not immediately removed the illegal content, as well as it has continued to publish it, even if the conditions provided for in Article 16 of Legislative Decree no. 70/2003 are met jointly.[1184]

In view of the political-social evolution and of the greater common awareness, it is believed that the legislation will take action in an increasingly predominant way in the control of Internet providers, also through the imposition of preventive controls inherent to the contents published on digital platforms.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

According to Article 21 of the Italian Constitution 'Anyone has the right to freely express their thoughts in speech, writing, or any other form of communication'. They are based on the freedom of thought. Fundamental and inalienable rights

[1180] In this regard, according to Article 17 of Legislative Decree 70/2003: 'The provider shall be civilly liable for the content of such services if, at the request of the judicial or administrative authority having supervisory functions, he/she has not acted promptly to prevent access to that content, or if, having been aware of the illegal or prejudicial nature of the content of a service to which he/she grants access, he/she has not informed the competent authority'. Therefore, the internet service provider is responsible in relation to the knowledge of the illegality of the information.

[1181] The judge of first instance had not qualified as a copyright infringement the broadcasting on the online platform of films taken from various television programs.

[1182] Although Italy is a country of Civil Law, the rulings of the Supreme Court serve as a precedent for the orientation of judicial activity; it seems reasonable to maintain that, unless there are sudden changes of orientation, the rulings of the courts will be based on the subsequent judgments cited herein.

[1183] The conclusions reached by the Court of Cassation, fully in agreement with those of the Jurisprudence of the Court of Justice of the European Union, will probably be considered outdated given the emanation of the new directive on Copyright of the European Parliament.

[1184] Furthermore, the judges stressed that for the purposes of correct identification the content of the appeal cannot be generic but, on the contrary, refer to specific URLs which thus becomes a necessary element.

could be in conflict with the Article 21, such as the right of publicity and personal reputation. They could be exposed by news reports or public importance news. Attempts have been made in order to avoid the use of online news to spread defamation. It is possible to have the content removed, according to the privacy rules and the protection of data of the Reg. UE/679/2019.[1185] The involved person has the right to ask the remove of news from the internet when they are wrong, inaccurate, false and/or outdated. Obsolescence and inaccuracy are the legal basis to ask the remove of a defamatory internet content. A false or wrong information is used to value if the news is defamatory or not. The Right to Privacy of the citizen is more important than the right to freedom of the online news. The Personal Data Code was drafted with the Legislative Decree n.196/2003, integrated with Legislative Decree n.101/2018.[1186] Many websites are blocked in Italy because they breached the copyright through the sharing of files with equal protocols (*protocolli paritetici*). Thanks to the action of Postal Police, National Center for the Fight Against Pedopornography and judicial authorities, 6400 websites are obscured since 2015.

The Authority to Guarantee Communications helped blocking more than 20 streaming websites and the Court of Rome [1187] commanded anti-piracy measures and asked to internet connection providers to limit the access to 24 streaming websites.

The European Commission, Member States, Europol, Global Internet Forum and internet service providers collaborate to ensure the protection of personal data and the removal of terrorist content online.[1188]

Terrorism is regulated by the Article 270 bis and following of the Criminal Code. As for as this research is concerned, the 'cyberterrorism' and the potentially terrorist material deal with the threat to public order, public security and national defence.

[1185] Known as the General Data Protection Regulation (GDPR)

[1186] Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of individuals with regard to the processing of personal data, as well as free movement of such data and repealing directive 95/46 / EC (General Data Protection Regulation).

[1187] Specialised Section for Intellectual Property of the Civil Court of Rome, on the request for precautionary measures proposed by FAPAV, the Audiovisual Anti-Piracy Federation vs. Telecom Italia.

[1188] Fight against online terrorism: The EU Internet Forum is committed to respecting an EU-wide crisis protocol, Brussels, 7th October 2019, pp. 1-2.

After the terrorist attacks in London and Madrid, an Antiterrorism Act has limited the opening of new hotspots and subjected them to request for permission to the Postal Police.[1189]

The crime of education or self-training aims to suppress criminal behaviour potentially achievable,[1190] for example by 'foreign fighters', that are people who go to another State for 'perpetration, planning or preparation of terrorist acts or providing or receiving terrorist training'[1191], given the increasing attention to episodes of radicalism and the use of the Internet to spread dangerous messages. According to the Supreme Court,[1192] downloading videos and documents from the Internet with a didactic value on the use of weapons and explosives to be used for the execution of terrorist acts of a jihadist matrix, is already, in itself, suitable to be configured as an unequivocal direct behaviour to achieve a crime-related fact that can be placed in Article 270-sexies.[1193]

In the Italian Civil Code, the Article 10 regulates the abuse of others' image: the judge, on request of the involved person, can command the abuse to stop and ask for the compensation for damages. The reproduction of an image is justified by fame, public office, need of justice, scientific, educational, cultural aims, exposure linked to public facts, events or ceremonies, public interest. Anyway, the expose should be correct, without outbursts, false and untrue reconstructions.

Defamation is a criminal offence and it is a damage to the right of reputation.[1194]

According to the most recent Italian doctrine and jurisprudence, it can take place through the internet, given the large use of it. The Supreme Court claimed 'The means of transmission-communication used (in this case, internet) allows, in the abstract, (also) the vilified person to perceive the offense directly'.[1195] The message, furthermore, is directed to such a large group of users, that the damage is in a wider dimension than the interpersonal one between offender and offended.

1189 Article 6 e fol. Law 31 July 2005, n. 55 "Conversion into law, with amendments, of the decree-law of 27th July 2005, n. 144, containing urgent measures to combat international terrorism", in the Official Gazette n. 177 of 1 August 2005.

1190 Article 270-quinquies Criminal Code.

1191 Security Council Counter-Terrorism Committee <https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters/> accessed 8 February 2020.

1192 Supreme Court, Section V pen., 19 July 2016, n. 6061.

1193 Pietro Maria Sabella, "Il fenomeno del cybercrime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali", (2017), Informatica e diritto, year 43, vol. 26, page 171

1194 Article 595 Criminal Code.

1195 Supreme Court, Criminal Division., section V, 16th October 2012, n. 44980; Supreme Court, Criminal Division, section V, 17th November 2000, n. 4741 <https://www.diritto.it/la-diffamazione-online/>.

Relevant Case about the removal of internet content (Right to be Forgotten): A known person asked the Privacy Guarantor, and then the judicial authority, to order a publisher of a newspaper to update an online article about his arrest, with the mention of his subsequent acquittal. The trial court (*giudice di merito*) declared that the publication of the news constituted a legitimate exercise of the right to report, because, at the time, the news was true and of public interest. The presence of the article in the online archive had a documentary function and there was no Right to be Forgotten, given the person's reputation. The Supreme Court, instead, recognised the person's Right to be Forgotten, considered 'the right to protect his (current) personal and moral identity in his social projection'.[1196] Keeping the online article is used for documentation purposes if it is updated and contextualised, otherwise it no longer corresponds to the truth and must be deleted. In the present case, there is an obligation for the publisher to set up a system to report the presence of news development and fast access to it. After this ruling, the Privacy Guarantor requested the editor to insert an annotation on the corner of the article when there is a 'continuation' of the reported news.[1197]

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

Online platforms are the main access point to information on the Internet, which has not only increased the volume and variety of issues available to people but has also transformed the ways in which they relate to them. Social networks have become *de facto* channels of information. Furthermore, on the web every user can become an actor of communication: Internet breaks the mould and allows anyone to express their opinion. This is the reason why it can be said that through the Web freedoms of expression and information are fully and concretely implemented, this allowed to make today's democracies more participatory and inclusive. However, this positive evolution was accompanied by phenomena of degeneration: the dissemination of targeted hate speech and large-scale disinformation propagation (fake news). If there is no doubt on the one hand that harmful conducts to the dignity of people are obstacles to civil coexistence, nevertheless actions aimed at containing and filtering the communications that take place on the Internet can translate into a limitation of

[1196] Diritto 24 Il Sole 24 ore <http://www.diritto24.ilsole24ore.com/civile/civile/primiPiani/2013/07/internet-e-diritto-alloblio-una-recente-sentenza-del-tribunale-di-milano.php> accessed 9 February 2020.

[1197] Supreme Court n. 5525/2012.

the principle of freedom of expression and become surreptitiously forms of censorship. On the other hand, the concept that these phenomena must be regulated by a law of a single State appears unsuitable to manage manifestations of thought that go beyond the boundaries of space and time: a more suitable approach based on self-regulation is undoubtedly preferable to adapt with sufficient flexibility to the rapid changes in the context and to the evolution of technologies.

In Italy, the issue has been felt and discussed for a long time considering the dangers for democracy from both the absolute lack of control and the imposition of State censorship. Already in 2010, a self-regulation Code for Internet Services was proposed containing rules of conduct for all network operators, from access providers to host providers who had signed it: all participating operators could have exhibited a quality certificate issued by the State to guarantee about the reliability of the contents. Critics followed that, they essentially focused on the fact that this State control system could turn into an indirect censorship tool based on the social credibility of online platforms without the certificate, so the attempt to stipulate this Code was negative. This self-regulation attempt was preceded by a more general Self-Regulation Code for the Internet Services in 1998 adopted by the Italian Internet Provider Association (AIIP) with the aim of preventing illicit or potentially offensive use of Internet by spreading a correct culture of responsibility by all subjects active on the Network. In particular, the objectives of the Code, which regulates the behaviour of the associated providers, are: to provide all the subjects of the Internet with rules of conduct in order to protect the human dignity (Article 6), to provide users of the Network with information and technical tools to use services and content more consciously, provide all parties on the Internet with an interlocutor to contact for reporting any cases of violation of this Code (Article 2). In summary, it is providing the possibility to send a report of infringements by Internet subjects (users and providers), after which the self-control body, after hearing the parties, decides on the basis of the instructor's report and of the deductions and/or documents filed by the parties by adopting measures eligible, so even the deletion of the content from the online platform (Article 13). In the end it states that any provider from AIIP will directly inform the judicial authority when it becomes aware of the existence of content accessible to the public of an illicit nature and that the self-control body should contact the judicial Authority ensuring the maximum collaboration for the investigations in case of reporting of illegal content or behaviour and in violation of the Code, so the providers have to inform the users about their right to suspend and block the dissemination of illegal content in application of the

notices of the judicial authority (Article 14). However, the low number of subjects involved, and the generality of the rules have made this instrument almost useless.

In conclusion, transparency on the part of providers, culture of legality, pluralism, literacy of information, education in knowledge and development paths of cognitive skills can represent the most suitable tools for finding ways to safeguard freedoms of expression and information, and allow for the fight against the spread of hate speech and disinformation, while avoiding technical and regulatory complaints that could jeopardise the implementation of freedom of expression. Today's tools are still inadequate considering the huge scale of the phenomenon, but the process of their effective development is underway.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

Italy does not have a specific legislation on the right to be forgotten. In the 90s the Italian doctrine started to discuss the nature of the right to be forgotten,[1198] influencing the legislator that introduced the Law 675/1996.[1199] In the Article 13 were disciplined the rights of the data subject, including the right to be forgotten or right to erasure: the article considered the power of the data subject to ask the upload and the erasure of incorrect or unlawful contents.[1200] The Law was abrogated by the Code of Privacy introduced by the Legislative Decree no. 196/2003.[1201] This was edited and reformed by the introduction of the General Data Protection Regulation.

Out of the legislative regulation, very poor as it was explained, the jurisprudence and the Italian Data Protection Authority Provisions played a huge role. Stefano Rodotà, Italian Data Protection Authority from 1997 to 2005, gave a definition

1198 F. Di Ciommo, Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio, in I dati personali nel diritto europeo, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Giappichelli Editore, Torino, 2019.

1199 L. 675/1996, Italian text, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/28335>.

1200 In the Article 13, par. 1 sub lett. C we can find the equivalent of the right to be forgotten, as shaped in the 90s by the Italian Legislator.

1201 The Code was amended by the Legislative Decree no. 101 of 10 august 2018, adapting the national legal system to the GDPR. Italian text, <https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.7>.

of right to be forgotten 'the right to repel the invasion in the private sphere and moreover the right to control the flux of information on a certain subject.' [1202]

It is a Right that cannot be always recognised, as it is necessary a balance with the Right to report, constitutionally protected by the Article 21 of the Italian Constitution, and, *ad abundantiam*, by the Article 2, as well.

Both the Court and the DPA tried to implement and to make the Right to be Forgotten effective. The latter one is committed in a capillary activity of 'check and balances', protecting the opposite interests of the two categories involved: people and journalists. One of the activities the DPA did, out of the numerous provisions[1203], was to provide Code of Conducts, including the one devoted to journalists about publishing and processing personal data, a bastion against illegal distributions.[1204]

The Italian Jurisprudence approached the Right to be Forgotten from different perspective and in wide occasions.[1205] In consideration of what is established by the code of conduct, the Italian Supreme Court considered that not every Right to Access Information is adequate to prevail on Right to Privacy. The Court established that the necessity of publication and the demand of protection of a data subject must be examined case by case in concrete, as it is not possible to define a rule based on a general amount of time in which a news can be considered not more interesting and relevant for the public society.[1206]

This is a contest of uncertainty, where there is not a sole guide to follow and to comply with on the issues related to the Right to be Forgotten. It can be defined as Ianus,[1207] a figure with two heads:one of general application at the European level and the other one operating at a national level. Both need to work together to find a common and coherent application and in particularly the domestic legislator needs to take a position on the topic in order to prevent equivocal and contradictory judgments and provisions.

[1202] Abstract of Stefano Rodotà's speech, presentation of the annual report, 2001, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3541955>.

[1203] Just to mention the Provisions about the relationship between recent news, data protection and right to report: Provvedimento del Garante n. 496 del 6 novembre 2014, Provvedimento n. 500 del 6 novembre 2014, Provvedimento n. 40 del 20 gennaio 2015, Provvedimento n. 326 del 28 maggio 2015, Provvedimento n. 342 del 4 giugno 2015.

[1204] Article 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 29 novembre 2018 [9067692].

[1205] Just to mention some of the judgments of the Court of Cassation: 13161/2016; 38747/2017; 28084/2018; 19681/19.

[1206] Judgment n. 16111/2013.

[1207] R. Pardolesi, L'ombra del tempo e (il diritto al)l'oblio, in Questione di Giustizia, Thrimestral Journal, 1/2017.

6. How does your country regulate the liability of internet intermediaries?

In Italy, the issue of internet intermediaries' liability has sparkled a jurisprudential and doctrinal debate aimed to find a balance between conflicting exigencies: on one side, the urgency to identify the responsible of unlawful acts in order to fulfil the claims for compensation of those who have unjustly suffered a damage; on the other, the necessity of not excessively burdening private subjects such as providers.[1208] In the Italian legal system, a key role is played by the Legislative Decree (LD) No. 70/2003 of 9 April 2003,[1209] which refers directly to the E-Commerce Directive.[1210] According to Articles 14, 15, 16 of the LD, internet service providers (ISPs) shall not be made liable in civil or criminal law for purely passively transferred information, even after having been given notice thereof:[1211] the responsibility dispensation exists as long as providers remain in a position of absolute neutrality in relation to the information conveyed. This exemption applies to all of the three different categories of internet intermediaries classified by the Legislative Decree: those providing mere conduit, caching and hosting services. However, caching and hosting service providers are obliged to carry out certain information and operational tasks which introduce their responsibility although they do not entail the obligation to examine in advance the information transmitted in order to evaluate their possible damage to third parties.[1212] Article 17.1 affirms that there is not a general obligation to monitor contents and clarifies that ISPs have no duty to carry out any active investigation into facts or circumstances that may indicate the presence of an illegal activity.[1213] Nevertheless, in any case where a caching service provider may know of allegedly illegal activity or information concerning the end-users of its services, it is required to collaborate with and inform the

[1208] Article 2043 of the Italian Civil Code affirms that: "Any person who by wilful or negligent conduct causes unfair detriment to another party must compensate that injured party for any resulting damage". In addition, Article 2055 refers to joint liability in the case where the unlawful act is committed by several persons.

[1209] Legislative Decree No. 70/2003 (implementing Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market) <http://www.interlex.it/testi/dlg0370.htm>, accessed 12 February 2020.

[1210] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN>, accessed 12 February 2020.

[1211] Specifically, as stated by Article 14 of the Legislative Decree No. 70/2003, mere conduits providers 'must not respond for the transfer of information on condition that they do not initiate the transmission, do not select the receiver of the transmission and do not select modify the information contained in the transmission'.

[1212] Legislative Decree no. 70/2003, Article 15.1(e), Article 16.1(b).

[1213] ibid, Article 17.1.

judicial and administrative authorities.[1214] Moreover, it has to be specified that the public prosecutor or judge of enquiry shall authorise the list of illegal content before blocking or takedown can proceed.[1215] Article 17.3 states that any ISP who fails to act promptly to bar access to the material following a request from a competent administrative or judicial authority in the course of its monitoring duties, will be held civilly liable. So, if the conditions set out in the Legislative Decree exist, intermediaries are not accountable for the unlawful acts committed by users using their services; if instead the providers do not comply with the rules, they become accountable. Recently, the Directive on Copyright in the Digital Single Market has envisaged a specific responsibility for online content sharing service providers (OCSSPs) in case of unauthorised acts of communication to the public, affirming that they are strictly liable for the content uploaded by users.[1216] In few words, the Directive targets to make OCSSPs responsible for the content they host together with those who share them,[1217] with the aim of protecting the works' copyright by avoiding unauthorised use for profit.[1218] Therefore, it is necessary to stress the role of these actors as facilitators of the exercise of the Right to Freedom of Expression.[1219] In this context, the Decision no. 31022, 2015 of the Italian Supreme Court of Cassation considered that guarantees provided by Articles 21.3, 21.4 of the Constitution are extensively applicable to the online press;[1220] that may consist in an obligation of ISPs to make the resource inaccessible.

Now, more than ever, legal tools must be timely adapted to fulfil the need of fundamental rights and freedoms' protection, constantly threaten by new challenges of the digital age.

1214 ibid, Article 15.1(e), Article 16.1(b).

1215 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015.

1216 Directive 2019/790/EU of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, that has not yet been implemented in the Italian legal system.

1217 ibid, Article 17(4).

1218 Unless the service providers demonstrate that they have respected the conditions listed by Article 17(4) of the Directive 2019/790/EU.

1219 Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, adopted by the Committee of Ministers on 7 December 2011 at the 1129th meeting of the Ministers' Deputies.

1220 Italian Supreme Court of Cassation, Decision no. 31022/2015: <https://www.penalecontemporaneo.it/upload/1437150339Cass_SU_31022_15.pdf>, accessed 12 February 2020.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

While on the right to be forgotten there will not likely be major legislative changes over the next years, the Italian Privacy Authority will continue to play an essential role to 'transpose' and spread the European principles in the national system – which will address the search engines deindexing and whether or not the Right to be Forgotten should be restricted within the Member States of the European Union.[1221]

With the approval of the new Directive on Copyright in the Digital Single Market,[1222] the role and responsibilities of online intermediaries and platforms have been reshaped within a sectoral approach. Although in Italy the Directive has not been implemented yet, we can expect it to have consequences.

From an intermediary liability perspective, the most relevant provision is Article 17 on 'Certain uses of protected content by online services'.

In case of violation of the obligation to obtain prior licensing agreements with right holders, Article 17 of the new Directive expressly excludes the provider of online services taking advantage of the exemption of liability provided by Article 14 of the 2000/31/EC directive (implemented in Italy in Legislative Decree no. 70/2003).[1223]

It should be stressed that the new Directive does not expressly provide - as it was in its original formulation - an obligation of preventive control (upload filter), but only a general obligation to obtain a license from the right holder in order to share revenues obtained from the uploading of content by users. However, the requirement for some online service providers to demonstrate to have made the maximum efforts to prevent the uploading of unauthorised works in the future will probably make necessary and essential the use of preventive filters by the Internet Service Providers, contradicting *de facto* the no-monitoring

[1221] See Case C-507/17 Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) Google has won a long-standing battle with the European Union, after the European Court of Justice ruled the company can limit the scope of the "right-to-be-forgotten" regulation to searches made within the EU.

[1222] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[1223] The Directive 2000/31/EC applies horizontally to any kind of illegal or infringing content.

obligation set out in Article 15 of the eCommerce Directive[1224] and confirmed by the CJEU.[1225]

This liability system makes notice (or knowledge) and take-down procedures irrelevant for copyright infringement, putting a spotlight on filtering and monitoring.[1226]

A privatisation of online enforcement through algorithms and based on privately enforced standards rather than transparent legal obligations could be a risk to fail a 'fair balance' between copyright

and other fundamental rights as users' freedom of expression;[1227] it remains to see how the national legislator will try to maintain the balance implementing the Directive.

Also, it will be up to the national legislator to clarify the scope of the licenses granted to the platforms, in fact they also involve the use of individuals who publish content for non-commercial purposes or whose activities do not generate significant revenues.

It will be necessary for the legislator to decide if intervene on the sanctioning power of the independent Guarantor Authority for the communications (AGCOM), since the Council of State has declared[1228] illegitimate the part of AGCOM Regulation[1229] concerning the possibility to put administrative sanctions on internet service providers not complying with blocking and removal orders of the administrative Authority, which has the power to order to block illegal activities.[1230]

The Council of State has sentenced to leave the sanctioning power to the judicial Authority and the legislator could decide – against the trend - to endorse this position, further undermining the administrative Authority role.[1231]

[1224] According to Article 15, Member States are not allowed to introduce obligations that would require intermediary service providers to systematically monitor the information they store or transmit.

[1225] See Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et editeurs SCRL (SABAM).

[1226] See Frosio, G. (2017) 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe, Journal of Intellectual Property Law and Practice 12(7) 565-575.

[1227] As clearly emerges from the Comparative Study on Blocking, Filtering and Take-down of illegal internet content provided by the Swiss Institute of Comparative Law ("SICL"), the danger of voluntary blocking or suppression of information by private actors is of concern to the Council of Europe.

[1228] Cons. St., sez. VI, 15 luglio 2019, n. provvedimento 201904993.

[1229] Resolution 680/13/CONS.

[1230] According to Articles 14-16 of the Legislative Decree no. 70/2003, AGCOM may require the service provider to inhibit 'harmful' activities. This power of intervention is also granted by the judicial Authority, which can also exercise it as a matter of urgency.

[1231] The small number of measures issued by AGCOM - compared to the number of infringements that can be found online - is not due to an inefficiency of the Authority, but probably from the limited

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

Regardless the fact that Italy was one of the signatories of the 2001 Budapest Convention (although the country has not ratified yet the 2003 Additional Protocol to the Convention, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems), no relevant legislation has yet been put in place on the national level to contrast hate speech whilst guaranteeing freedom of expression online in a way which is consistent with the fundamental rights granted by the national Constitution. Notwithstanding the complete absence of a comprehensive and effective response by the Italian government and other institutions, drastic resolutions have been adopted to oppose the deterioration in the tone of public debate. In 2016, the Chamber of Deputies established a Special Parliamentary Committee on Intolerance, Xenophobia, Racism and Hate to gather data, take evidence from experts and stakeholders, and formulate concrete normative proposals to counter the phenomenon. What came out from this work is a series of recommendations which call for a number of regulatory interventions and the adoption of policies, touching upon societal, cultural, educational and media-related elements.[1232] Among the actions proposed, the Committee outlined the necessity to adopt a legally recognised definition of 'hate speech' based on the definition given by the ECRI in Recommendation no. 15, adopted on 8 December 2015, as well as to reinforce the mandate of UNAR (*Ufficio Nazionale Antidiscriminazioni Razziali,* Italy's anti-racial discrimination departments), which has been involved, through the National Media and Internet Observatory, in monitoring and analysing potentially discriminatory content online. A previous attempt to tackle the matter, with regards to communications on the Internet, could be found in the work of the Special Parliamentary Committee to study the rights and duties of the Internet, previously established by the Chamber of Deputies in 2014, which led to a 'Declaration of the rights on the Internet', a framework policy document with which all legislators, institutions, Internet operators and users should comply, though it is not legally binding. Article 13, par. 2, of the Declaration expressly provides that 'no limitations of freedom of

knowledge of the instrument by rightsholders, even considering that AGCOM cannot initiate proceedings on its own initiative, but acting only on the request of the interested party.

[1232] Chamber of Deputies, Recommendations of the "Jo Cox" Committee on Intolerance, Xenophobia, Racism and Hate, approved on 6 July 2017 <https://www.camera.it/application/xmanager/projects/leg17/attachments/uploadfile_commissione_intolleranza/files/000/000/004/Raccomandazioni_lug17_EN.pdf> accessed 5 February 2020.

expression are accepted' online, but 'the protection of people's dignity must be protected from abuses related to behaviours such as incitement to hatred, discrimination and violence'.[1233] The activity carried out by these Special Parliamentary Committees is commendable, but shows an evident lack of perspective as to the necessary tools and remedies to be introduced within the legal framework to contrast this growing concern. Ultimately, the Senate has recently passed a motion to set up an extraordinary commission against hate, racism and antisemitism, a clear sign that more has to be done at the institutional level to overcome the atmosphere of violence and hate that seems to be spreading across the country.

8.1. Positive measures recommended to comply with international standards

What emerges from the analysis is an acute awareness of the problem, accompanied by plenty of initiatives launched to reverse the trend, which have not resulted into any practical solutions in terms of laying the foundations of new *ad hoc* laws and implementing the existing ones, governing several crucial aspects of freedom of expression in relation to hate speech. This is the case, among the others, of the Law no. 112/2004 (*i.e. Gasparri Law*), followed by the Legislative Decree no. 177/2005 (Consolidated Act on Radio and Audiovisual Media Services), which outlined the basic principles applicable to radio and audiovisual media services: the Consolidated Act especially prescribes that no provider under Italian jurisdiction may disseminate content with 'any incitement to hatred however motivated or leading to attitudes of intolerance based on differences of race, sex, religion or nationality',[1234] and the same obligation applies to commercial communications (e.g. advertisements and telesales) aired by these subjects.[1235] Similar rules shall be representing the starting point to fulfil the commitments undertaken to prevent and counteract hate speech online on an international basis. In fact, it is visible here the willingness to cooperate with the private sector towards the engagement in censorship of offensive content without any independent adjudication on its legality: some viable options in this sense are offered by the 2016 European Commission's Code of Conduct on Countering Illegal Hate Speech, which stresses the need to defend the Right to Freedom of Expression, 'applicable not only to "information" or "ideas" that

[1233] Chamber of Deputies, Declaration of the Rights on the Internet, adopted by the Committee for the Rights and Duties of the Internet on 28 July 2015 <https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf>, accessed 5 February 2020 [Italian].

[1234] Legislative Decree no. 177 of 31 July 2005 (Consolidated Act on Radio and Audiovisual Media Services), Article 4(1), letter b).

[1235] ibid, Article 4(1), letter c).

are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population'.[1236] This is something the Italian legislator must bear in mind for a potential legislative strategy responding to hate speech in all of its forms and in line with the international human rights obligations, to be discussed and approved by all relevant stakeholders, including not only State institutions, but also civil society organisations and IT operators. Therefore, as a conclusion on this theme, we could definitely say that Italy must continue on the path followed by the Special Parliamentary Committees and therefore take appropriate steps towards policies ensuring a fair control of the use of platforms such as the social media in a manner that keeps freedom of expression largely intact, whilst actively fighting against the use of hate speech by promoting diversity and inclusion of minorities through the guarantee of their adequate access to those platforms. Still, this is just one feature of a much bigger and more complex dispute on media pluralism which requires more than just a deep perception of this particular situation, a radical change in the national climate for political discourse.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

Considering the current relevance of the freedom of expression online and the balance between this main legal topic and the protection of other fundamental rights, such as human rights, intellectual property rights and information rights I would say that Italy has not already reached an adequate balance.

The Freedom of Expression is one of 'the pillars of democracy'[1237] and a right guaranteed by Article 21[1238] of the Italian Constitution at national level, by Article 10 CEDU[1239] at European level and by Article 19[1240] of Universal Declaration of Human Rights at international level. Taking into consideration the Italian constitutional law, it does not give a clear definition of the content and there is also no definition of the right of information, which is now relevant just because

[1236] European Commission, Code of Conduct on Countering Illegal Hate Speech Online, signed on 31 May 2016, page 1 <https://ec.europa.eu/info/sites/info/files/code_of_conduct_on_countering_illegal_hate_speech_online_en.pdf>, accessed 7 February 2020.
[1237] C. Cost., 17/04/1969 n. 84.
[1238] Article 21 Italian Constitution 1948.
[1239] Art 10 European Convention on Human Rights 1950.
[1240] Art 19 Universal Declaration of Human Rights 1948.

of the expansive interpretation of the Article 21.[1241] According to the growing and the potential of the Internet, freedom of expression has gained much importance. At the same time, the human rights obligations have gained new dimensions.[1242]

Starting from the principle 'what applies offline also applies online'[1243] we could say that also the Italian national law has felt the need to a new implementation and a new and adequate balance between a freedom that allows and guarantees pluralism and the protection of other rights.

The right of information is the starting point of one of the biggest issues of our 'online society'; fake news.[1244] Today everyone in every moment can find every type of information, using online newspapers but also a lot of blogs and social networks. Obviously, they are useful because of the spontaneity and immediacy of the information, but on the other hand, these news and articles often are not verified. According to P. Barile[1245] The diffusion of fake news could not be considered an unlawful act if it does not prejudice a constitutional value. For example, a value about reputation and privacy. In the Italian legal system, the diffusion of fake news is not unlawful per se, but only when it hurts public order. This is what Article 656 of the Criminal Code provides.[1246] Also, the Italian Constitutional Court considers the public order as one of the main values of our society, so we need to observe it and respect it if we want to have a juridical order.[1247]

A recent bill tried to introduce the punishment of who shares fake news, even if he is not an official journalist.[1248] The draft laws also introduced the liability of network providers that had the role to control websites and web platforms. Is it censorship? And, more important, is it compatible with the Rights of Freedom of Expression? Article 21 could be defined as a law that clearly belongs to the past and even if it is not easy to modify it and this may not be the right solution.[1249] Maybe we should start from a clear interpretation.[1250]

1241 M.Orofino, "Article21 Cost: le ragioni per un intervento di manutenzione ordinaria" [2008].

1242 Wolfgang Benedek and Matthias C. Kettemann "Freedom of Expression and the Internet", Council of Europe.

1243 Wolfgang Benedek and Matthias C. Kettemann, "Freedom of Expression and the Internet", Council of Europe.

1244 Giuseppe Laganà, Diritto dell'informatica.it "I profili legali delle fake news" [2017] <http://www.dirittodellinformatica.it/ict/crimini-informatici/profili-legali-delle-fake-news.html>.

1245 pageBarile, "Diritti dell'uomo e libertà fondamentali" [1984].

1246 Art 656, Italian Criminal Code [1930].

1247 C.Cost. 1962 n.9.

1248 Bill n.2688 "Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica" [2017].

1249 M.Orofino, "Article21 Cost: le ragioni per un intervento di manutenzione ordinaria" [2008].

1250 F. Donati "L'art 21 della Costituzione 70 anni dopo" [2018].

To overcome these critical issues (hate-speech, fake-news), between 2006 and 2008 there was a real Internet Rights Declaration. This was also reproduced in Italy by the Commission for Internet Rights and Duties and it was finally published on July 28, 2015.[1251]

Another problem, linked with the Right of Information, is that the network information economy is controlled by gatekeepers like Google with all the advertising profiling cookies managed directly by the website owner, defined in Article 4 of GDPR.[1252]

Italy has adapted to European provisions, but there is still a lot of work to be done, in order to have a legal system that responds to the new needs and that can balance our constitutional rights, that came from our national history, with the new world of Internet and Social Networks. Maybe we should start considering these issues not like something new and totally different from the law we are used to , but just as a bigger, freer world to rule, obviously with all the problems this brings.

10. How do you rank the access to freedom of expression online in your country?

Concerning freedom of expression online, Italy could be ranked as a 4 out of 5.

Italian government and other public authorities do not use censorship as a political tool to restrain freedom of expression and, overall, free speech is widely guaranteed both online and on other traditional media.

In particular, freedom of expression is guaranteed by Article 21.1 of the Italian Constitution,[1253] according to which everyone has the Right to freely express their ideas. According to Article 21.2, moreover, the press is free and cannot be restricted by censorship.[1254] For this reason, according to Italian Constitutional law, any law enacted by the Parliament or the Government that interferes with freedom of expression can be scrutinised by the Constitutional Court and expelled from the national body of laws. Moreover, Italy has signed the European Convention on Human Rights, and is thus bound by Article 10 of the

[1251] Declaration of Internet Rights [2015].

[1252] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[1253] Article 21.1, 'everybody has the right to freely express his own thoughts by words, writings and any other means of communication'.

[1254] Article 21.2, 'the press cannot be subject to preventive authorization and cannot be censored'.

Convention, stating that freedom of expression can only be restricted for specific reasons and having regard to the principles of proportionality and necessity.

Despite this, some national provisions might in some cases present a threat to individuals' freedom of expression, especially for what concerns the risk of being accused of libel, and the possibility of being restricted to express one's opinion online due to the block or removal of digital content on the web.

11. How do you overall assess the legal situation in your country regarding internet censorship?

Overall, Italian legislation regarding internet censorship strikes a good balance between freedom of expression and protection of the public interest. Some criticism however persists.

On one side, citizens might be refrained by expressing their own opinions because of the fear of civil lawsuits for 'libel' or 'aggravated libel through the press' under Article 595 of the Italian Criminal Code. In 2017 the Human Rights Committee of the UN issued an observation regarding the Italian provision on defamation, raising some concerns about the fact that 'forms of expression including defamation, libel and blasphemy remain criminalised including with punishment of imprisonment'.[1255]

On the other hand, even if Italian authorities do not engage in online censorship for political, social or religious reasons, Italy can be said to engage in selective internet filtering. Such practices are limited to the most serious legal violations, such as terrorist activities, child pornography, illegal gambling and infringement of intellectual property rights. According to the *Osservatorio sulla censura di Internet in Italia* (the Italian observatory for online censorship), at date Italy restricts the access to 6419 websites.[1256] Despite the fact that filtering is prescribed by law and can only be ordered in specific circumstances, concerns have been raised especially because blocking orders can be emanated even in the absence of a previous judicial decision and without the guarantees of a due process. In fact, of the 6419 censored websites, only 671 were blocked following an order of a judicial Court.

[1255] Concluding observations on the sixth periodic report of Italy," United Nations, Human Rights Committee, March 2017.

[1256] Internet censorship observatory in Italy <https://censura.bofh.it> accessed 11 February 2020.

Several legal tools grant independent administrative bodies the power of issuing blocking or take-down orders both to the Internet Service Providers and to the Internet Host Providers, depending on the circumstances.

Following the UN Resolution n. 2178/2014, the government enacted the decree 7/2015 (now law 17 April 2015, n. 43) prescribing urgent legislative measures for countering terrorism.[1257] Article 2 of this decree enables the Public Prosecutor and the Police to include websites that have a relation with terrorist organisations into a specific blacklist. The ISPs then have then the obligation to block the access to such websites.[1258] This law has been criticised *inter alia* for having broadened the definition of terrorism in the Italian criminal code, thus allowing for potential restriction on free speech.[1259]

A similar system is in place for countering child pornography and child abuse.[1260] The law 6 February 2006 n. 38 grants the National Center for the Countering of Online Child Pornography the duty-power to compile and keep updated a blacklist of websites hosting pedopornographic material. The ISPs have the duty to monitor such blacklist, and to take any measure to ensure that the access to these websites is precluded from the public.

Recently, the law 29 May 2017 n. 71 has also introduced a procedure for the removal of any content related to cyberbullying.[1261] According to article 2 of this law, it is possible to file a complaint either directly to the webmaster, to the host provider or to the Authority for the Protection of Personal Data, in order to request the removal of any content related to hate speech online against children and teenagers under age.[1262]

The most problematic piece of legislation, however, is the resolution enacted in 2014 by the Italian Authority for Communications Guarantees (AGCOM).[1263] Such resolution grants the Authority the power to issue to ISPs administrative blocking orders for website containing copyright violations,[1264] even in the

[1257] On cyberterrorism see G. Ziccardi, *L'odio online* (Raffaello Cortina Editore, 2016), 147.

[1258] See L. V. Berruti, Blacklist e blocco dei contenuti web illeciti: dal contrasto alla pedopornografia al cyber terrorism. Commento al d.l. 7/2015, Article 2, in Legislazione penale, 15.01.2016.

[1259] M.C. Amorosi, Terrorismo, diritto alla sicurezza e diritti di libertà: una riflessione intorno al decreto legge n. 7 del 2015, in Costituzionalismo, fasc. 2, 2015.

[1260] M. Faccioli, Minori nella rete. Pedofilia, pedopornografia, deep web, social network, sexting, gambling, grooming e cyberbullismo nell'era digitale (Key Editore, 2015) 27.

[1261] On cyberbullying in Italy see G. Ziccardi, *L'odio online* (Raffaelo Cortina Editore, 2016), 205.

[1262] page Pittaro, La legge sul cyberbullismo, in Famiglia e diritto, 2017, 819; R. Bocchini, Le nuove disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, in Nuove leggi civili commentate, 2018, 340.

[1263] AGCOM, Resolution n. 680/13/CONS.

[1264] On this topic see L.C. Ubertazzi (ed.), *Il Regolamento AGCOM sul diritto d'autore* (Giappichelli, 2014).

absence of any investigation by national Courts.[1265] With the decision 30 March 2017 n. 04101, the Regional Administrative Tribunal of the Lazio Region found the resolution to be compatible with the law.[1266]

Concerning the Right to Information, it is not explicitly recognised by the legislation, but the Italian Constitutional Court in 1994 stated that it immediately derives from the Freedom of Expression, and that the State must promote external pluralism to its greatest extent in order to satisfy the citizens' Right to Information.[1267]

Finally, although there is not a general legislative provision regulating the 'right to be forgotten' (*diritto all'oblio)*, such a Right now finds limited recognition in the General Data Protection Regulation. The jurisprudence however has ruled in favour of a more general Right to be Forgotten in several national cases,[1268] and now follows the interpretation provided by the CJEU in the Google Spain case.[1269]

[1265] See F. Piraino, Spunti per una rilettura della disciplina giuridica degli internet service provider, in AIDA 2017, 468.

[1266] See M. Renna, Le questioni di legittimità del regolamento dell'AGCOM sulla tutela del diritto d'autore online, in AIDA 2014, 111; C. Alvisi, La protezione dell'Agcom degli interessi contrapposti ai titolari, ibid. 163; F. Goisis, Profili di legittimità nazionale e convenzionale europea della repressione in via amministrativa delle violazioni del diritto d'autore sulle reti di comunicazione elettronica: il problema dell'enforcement, ibid. 180.

[1267] See the decision of *Corte Costituzionale* 7 December 1994, n. 420, and in general F. Bassan, E. Tosi (Eds.), *Diritto degli audiovisivi* (Giuffrè, 2012).

[1268] See for instance the decision no. 23771/2015 of the civil court of Rome.

[1269] CJEU, Cause C-131/12 – Google Spain SL, Google Inc./ Agencia Española de Protección de Datos, Mario Costeja Gonzále.

Table of legislation

Provision in Italian	**Corresponding translation in English**
Decreto Legislativo 70/2003 Article 15 (Responsabilità nell'attività di memorizzazione temporanea - caching) 1. Nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che: a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni; e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione. 2. L'autorità giudiziaria o quella amministrativa aventi funzioni di vigilanza può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse. Article 16 (Responsabilità nell'attività di memorizzazione di informazioni - hosting-)	Legislative Decree 70/2003 Article 15 (Responsibility for temporary storage - caching) 1. In the provision of an information society service consisting of the transmission, over a communications network, of information provided by a recipient of the service, the provider shall not be liable for the automatic, intermediate and temporary storage of such information carried out for the sole purpose of making its subsequent transmission to other recipients at their request more efficient, provided that: (a) it does not modify the information; (b) it complies with the conditions for access to the information; (c) it complies with the rules for updating the information, indicated in a manner widely recognised and used by undertakings in the sector; (d) does not interfere with the lawful use of technology widely recognised and used in the industry to obtain data on the use of the information; (e) act promptly to remove the information it has stored, or to disable access to it, as soon as it becomes aware that the information has been removed from its initial location on the network or that access to the information has been disabled, or that a court or administrative authority has ordered its removal or disabling. 2. A judicial or administrative authority having a supervisory role may require, even as a matter of urgency, that the provider, in the exercise of the activities referred to in paragraph 1, prevent or bring to an end infringements committed. Article 16 (Responsibility in the activity of information storage - hosting-)

1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.	1. In the provision of an Information Society service consisting of the storage of information provided by a recipient of the service, the provider shall not be liable for the information stored at the request of a recipient of the service, provided that that provider: (a) is not actually aware that the activity or information is unlawful and, as regards actions for damages, is not aware of facts or circumstances which make it apparent that the activity or information is unlawful; (b) as soon as it becomes aware of such facts, upon notification by the competent authorities, take immediate action to remove the information or to disable access to it.
2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore.	2. The provisions of subparagraph 1 shall not apply where the recipient of the service acts under the authority or supervision of the provider.
3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse.	3. The competent judicial or administrative authority may, even as a matter of urgency, require the provider, in the exercise of the activities referred to in subparagraph 1, to prevent or bring to an end infringements committed.
Article 17 (Assenza dell'obbligo generale di sorveglianza)	Article 17 (Absence of the general obligation of supervision)
1. Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.	1. When providing the services referred to in Articles 14, 15 and 16, the provider shall not be subject to a general obligation to monitor the information which it transmits or stores, nor to a general obligation actively to seek facts or circumstances indicating illegal activities.
2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto: a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo	2. Without prejudice to the provisions of Articles 14, 15 and 16, the provider shall in any event be bound: (a) to inform without delay the judicial or administrative authority responsible for supervision if he has knowledge of suspected illegal activities or information concerning a recipient of the Information Society service;

destinatario del servizio della società dell'informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite. 3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente.	(b) supply without delay, at the request of the competent authorities, the information in its possession enabling it to identify the recipient of its services with which it has data storage arrangements, in order to detect and prevent unlawful activities. 3. The provider shall be civilly liable for the content of such services if, at the request of the judicial or administrative authority having supervisory functions, it has not acted promptly to prevent access to that content, or if, having been aware of the unlawfulness or harmfulness to a third party of the content of a service to which it grants access, it has failed to inform the competent authority thereof.
Codice di autoregolamentazione per i servizi Internet, Article 2: Il Codice di autoregolamentazione per Internet (di seguito Codice) ha l'obiettivo di prevenire l'utilizzo illecito o potenzialmente offensivo della Rete attraverso la diffusione di una corretta cultura della responsabilità da parte di tutti i soggetti attivi sulla Rete. Article 6: I fornitori di contenuto si obbligano: 1. a rendere facilmente accessibili in linea con ogni mezzo idoneo, compresa la posta elettronica, le informazioni circa le caratteristiche tecniche, le modalità di funzionamento e gli strumenti per l'utilizzazione dei programmi di filtraggio. 2. ad eseguire una autoclassificazione dei propri contenuti in base al sistema di classificazione riconosciuto come standard dal Codice e ad accettare le variazioni alle proprie classificazioni eventualmente richieste da parte dell'organismo di autodisciplina.	Self-regulation code for Internet services, Article 2: The Self-regulation Code for the Internet (hereinafter the Code) has the objective of preventing the illicit or potentially offensive use of the Network by spreading a correct culture of responsibility by all the subjects active on the Network. Article 6: Content providers commit themselves: 1. to make easily accessible online with any suitable means, including e-mail, information about the technical characteristics, operating methods and tools for using the filtering programs. 2. to perform a self-classification of its contents based on the classification system recognised as standard by the Code and to accept the changes to its classifications possibly requested by the self-regulatory body.
Article 14: Nel caso di segnalazione di contenuti o comportamenti che risultino, oltre che in violazione del presente Codice, pure illeciti,	Article 14: In the case of reporting content or conduct that is not only in violation of this Code, but also illegal, the Jury addresses the judicial

il Giurì si rivolge direttamente all'Autorità giudiziaria garantendo la massima collaborazione per il proseguo delle indagini. I fornitori di servizi informano i loro clienti della loro facoltà di sospendere e bloccare la diffusione dei contenuti illeciti in applicazione degli avvisi dell'Autorità giudiziaria.	authority directly, guaranteeing maximum collaboration for the continuation of the investigations. Service providers inform their customers of their right to suspend and block the dissemination of illegal content in application of the notices of the judicial authority.
Article *21* Costituzione Italiana: Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.	Article *21* Italian Constitution: Anyone has the right to freely express their thoughts in speech, writing, or any other form of communication.
Article 13 sub lett. c: 1. In relazione al trattamento di dati personali l'interessato ha diritto: c. di ottenere, a cura del titolare o del responsabile, senza ritardo: […] 2) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;	Article 13 sub lett. c: 1. With referral to the processing of personal data, the concerned party has the right: c. to obtain by the person responsible, without any delay: […] 2) the erasure, the anonymisation or the block of data processed unlawfully, included the ones of which the conservation is not needed in relation to the aims of the collection and the processing;
Codice Civile Italiano, articolo 2043: Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.	Italian Civil Code, Article 2043: Any person who by wilful or negligent conduct causes unfair detriment to another party must compensate that injured party for any resulting damage.
Corte di Cassazione Italiana, Sentenza n. 31022/2015. "La testata giornalistica telematica, in quanto assimilabile funzionalmente a quella tradizionale, rientra nel concetto ampio di stampa e soggiace alla normativa, di rango costituzione e di livello ordinario, che disciplina l'attività d'informazione professionale diretta al pubblico"; "Il giornale on line, al pari di quello cartaceo, non può essere oggetto di sequestro preventivo, eccettuati i casi tassativamente previsti dalla legge, tra i quali non è compreso il reato di diffamazione a mezzo stampa".	Italian Supreme Court of Cassation, Decision no. 31022/2015 "The online press, as functionally similar to the traditional one, falls within the broad concept of press and is subject to legislation, of constitution rank and ordinary level, which regulates the professional information activity directed to the public"; "The online press, like the offline one, cannot be subject to precautionary seizure, except in cases strictly provided by law, among which the crime of defamation in the press is not included".

Dichiarazione dei diritti in Internet, Articolo 13: 1. La sicurezza in Rete deve essere garantita come interesse pubblico, attraverso l'integrità delle infrastrutture e la loro tutela da attacchi, e come interesse delle singole persone. 2. Non sono ammesse limitazioni della libertà di manifestazione del pensiero. Deve essere garantita la tutela della dignità delle persone da abusi connessi a comportamenti quali l'incitamento all'odio, alla discriminazione e alla violenza.	Declaration of the Rights on the Internet, Article 13: 1. Security online must be guaranteed as a public interest, through the integrity of the infrastructure and their protection from attacks, as well as an individual interest. 2. No limitations of freedom of expression are accepted. The protection of people's dignity must be protected from abuses related to behaviours such as incitement to hatred, discrimination and violence.
Decreto Legislativo 31 Luglio 2005, n. 177 (Testo Unico dei servizi di media audiovisivi e radiofonici), Articolo 4: 1. La disciplina del sistema radiotelevisivo, a tutela degli utenti, garantisce: … b) la trasmissione di programmi che rispettino i diritti fondamentali della persona, essendo, comunque, vietate le trasmissioni che contengono messaggi cifrati o di carattere subliminale o incitamenti all'odio comunque motivato o che inducono ad atteggiamenti di intolleranza basati su differenze di razza, sesso, religione o nazionalità o che, anche in relazione all'orario di trasmissione, possono nuocere allo sviluppo fisico, psichico o morale dei minori o che presentano scene di violenza gratuita o insistita o efferata ovvero pornografiche, salve le norme speciali per le trasmissioni ad accesso condizionato che comunque impongano l'adozione di un sistema di controllo specifico e selettivo; *c)* la diffusione di trasmissioni pubblicitarie e di televendite leali ed oneste, che rispettino la dignità della persona, non evochino discriminazioni di razza, sesso e nazionalità, non offendano convinzioni religiose o ideali, non inducano a comportamenti pregiudizievoli per la salute, la sicurezza e l'ambiente, non possano arrecare pregiudizio morale o fisico a minorenni, non siano inserite nei cartoni animati destinati ai bambini o durante la trasmissione di funzioni religiose e siano riconoscibili come tali e distinte dal resto dei programmi con	Legislative Decree no. 177 of 31 July 2005 (Consolidated Act on Radio and Audiovisual Media Services), Article 4: 1. The discipline of the radio and broadcasting system, in order to protect users, guarantees: … b) the transmission of programs which respect fundamental human rights, being, however, prohibited those transmissions that contain any encrypted messages or in a subliminal nature or any incitement to hatred however motivated or leading to attitudes of intolerance based on differences of race, sex, religion or nationality or that, also in relation to the broadcast time, could harm the physical, psychic and moral development of minors or that present scenes of gratuitous, persistent or brutal violence or pornographic, without prejudice to special rules for conditional access transmission which however impose the adoption of a system of specific and selective control; c) the diffusion of advertising transmissions as well as fair and honest telesales, which respect the dignity of the person, do not evoke discriminations of race, sex and nationality, do not offend religious beliefs or ideals, do not encourage harmful behaviours to health, security and the environment, cannot cause moral or physical injury to minors, are not inserted in cartoons intended for children or during the transmission of religious services and are recognisable as such as well as distinct from

mezzi di evidente percezione, con esclusione di quelli che si avvalgono di una potenza sonora superiore a quella ordinaria dei programmi, fermi gli ulteriori limiti e divieti previsti dalle leggi vigenti; …	the rest of the program by means of clear perception, with the exclusion of those make us of a superior sound power than the ordinary one of programs, without prejudice to the additional limits and prohibitions set by applicable laws; …
Article 595 c.p. Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro.	Article 595 of the Italian criminal code Whoever, outside the cases of the preceding article, by communicating with other persons harms the reputation of a third person, can be punished with up to one year of imprisonment or with a fine up to 1032 euros.
Articolo 2.2 d.l. 18 febbraio 2015, n. 7. Ai fini dello svolgimento delle attività di cui all'articolo 9, commi 1, lettera b), e 2, della legge 16 marzo 2006, n. 146, svolte dagli ufficiali di polizia giudiziaria ivi indicati, nonché delle attività di prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo, di cui all'articolo 7-bis, comma 2, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, fatte salve le iniziative e le determinazioni dell'autorità giudiziaria, aggiorna costantemente un elenco di siti utilizzati per le attività e le condotte di cui agli articoli 270-bis e 270-sexies del codice penale, nel quale confluiscono le segnalazioni effettuate dagli organi di polizia giudiziaria richiamati dal medesimo comma 2 dell'articolo 7-bis del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005.	Article 2.2 law decree 18 February 2015, n. 7 For the purposes of carrying out the activities referred to in Article 9.1, letter b) and 9.2 of the law 16 March 2006, n. 146, performed by the police officers mentioned there, and for the activities prevention and repression of terrorist activities, referred to in Article 7-bis.2 of the law-decree 27 July 2005, no. 144, converted into law 31 July 2005, no. 155, the organ of the Ministry of the Interior for the Security and the Regularity of the telecommunications services, subject to initiatives and determinations of judicial authority, constantly updates a list of websites used for the activities described in articles 270-bis and 270-sexies of the criminal code, in which are listed all the reports made by the police officers described by Article 7-bis of the law-decree 144 of 2005, converted, with modifications, into the Law 155 of 2005.
Articolo 6 dell'Allegato A alla delibera AGCOM n. 680/13/CONS del 12 dicembre 2013. Qualora ritenga che un'opera digitale sia stata resa disponibile su una pagina internet in violazione della Legge sul diritto d'autore, un soggetto legittimato può presentare	Article 6 of the Attachment A to the Resolution of AGCOM no. 680/13/CONS of 12 December 2013. Whereas they believe that a digital work has been made available on an internet page in violation of the Copyright Act, the copyright

un'istanza all'Autorità, chiedendone la rimozione.	owner may file an application to the Authority, requesting its removal.

Bibliography

English titles

Legislation

Directive 2000/31/EC

Legislative Decree 70/2003

Reg. UE/679/2019 known as General Data Protection Regulation (GDPR);

Legislative Decree n.196/2003, integrated with Legislative Decree n.101/2018;

Law 31st July 2005, n. 55

Italian Criminal Code.

Legislative Decree 10th August 2019, n.101;

Legislative Decree 30th June 2003, n.196;

Code of conduct related to the processing of personal data in the exercise of journalistic activities published according to the Article 20, par 4, in d.lgs. 10th August 2018, n. 101 – 29th November 2018 [9067692];

Protection of people and other subjects on the processing of personal data, Law 675/1996;

Directive 2000/31/EC of the European Parliament and of the Council.

Directive 2019/790/EU of the European Parliament and of the Council.

Council of Europe Publication, Comparative Study on Blocking, Filtering and take-down of Illegal Internet Content, 20 December 2015.

Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, adopted by the Committee of Ministers on 7 December 2011 at the 1129th meeting of the Ministers' Deputies.

Legislative Decree no. 177 of 31 July 2005 (Consolidated Act on Radio and Audiovisual Media Services), available online at:
<https://www.camera.it/parlam/leggi/deleghe/testi/05177dl.htm>.

European Convention on Human Rights 1950

Universal Declaration of Human Rights 1948

Declaration of Internet Rights 2015

EU General Data Protection Regulation (GDPR) 2016

Reports

Fight against online terrorism: The EU Internet Forum is committed to respecting an EU-wide crisis protocol, Brussels, 7th October 2019.

Comparative Study on Blocking, Filtering and Take- down of illegal internet content provided by the Swiss Institute of Comparative Law ("SICL")

- Article 19, Italy: Responding to hate speech', 2018 Country Report, available online at: < https://www.article19.org/wp-content/uploads/2018/04/Italy-Responding-to-%E2%80%98hate-speech%E2%80%99_3.4.pdf>, accessed 27 January 2020.

- Chamber of Deputies, Recommendations of the Jo Cox Committee on Intolerance, Xenophobia, Racism and Hate, approved on 6 July 2017, available online at: <https://www.camera.it/application/xmanager/projects/leg17/attachments/uploadfile_commissione_intolleranza/files/000/000/004/Raccomandazioni_lug17_EN.pdf> , accessed 28 January 2020.

Wolfgang Benedek and Matthias C. Kettemann "Freedom of Expression and the Internet", Council of Europe.

Books

F. Di Ciommo, Right to erasure, right to the limitation to the processing and the right to be forgotten, in Personal data in the European Law, edited by V. Cuffaro, R. D'Orazio, V. Ricciuto, Giappichelli Editore, Turin, 2019.

Periodicals

Pietro Maria Sabella "The phenomenon of the cybercrime in the contemporary legal space. Prevention and repression of Criminal offences related to the use of Internet for terrorism purposes, between security needs and respect for fundamental rights" (2017), Information technology and law, yr. 43, vol. 26.

R. Pardolesi, The shadow of the time and the (right) to be forgotten, in in Questione di Giustizia, Quarterly Journal, 1/2017.

Frosio, G. (2017) 'From Horizontal to Vertical: An Intermediary Liability Earthquake in Europe, Journal of Intellectual Property Law and Practice 12(7) 565-575.

Digital resources

<https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters/>;

<https://www.cyberlex.net>

<https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf>

<https://ec.europa.eu/info/sites/info/files/code_of_conduct_on_countering_illegal_hate_speech_online_en.pdf>

Case law

Judgment No. 7708 of 2019 of the Court of Cassation

Specialized Section for Intellectual Property of the Civil Court of Rome, on the request for precautionary measures proposed by FAPAV, the Audiovisual Anti-Piracy Federation vs. Telecom Italia;

Supreme Court, Section V pen., 19th July 2016, n. 6061;

Supreme Court, Criminal Division., section V, 16th October 2012, n. 44980; Supreme Court, Criminal Division, section V, 17th November 2000, n. 4741;

Supreme Court n. 5525/2012.

Judgments by the Italian Court of Cassation:

16111/2013;

13161/2016;

38747/2017;

28084/2018;

19681/2019.

Italian Supreme Court of Cassation, Decision no. 31022/2015.

Scarlet Extended SA vs Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10);

Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (C-507/17)

CJEU, Cause C-131/12 – Google Spain SL, Google Inc./ Agencia Española de Protección de Datos, Mario Costeja Gonzále

Italian Constitutional Court, decision 7 December 1994, no. 420

Civil Court of Rome, decision no. 23771/2015.

Italian titles

Legislation

Direttiva 31/2000 CE

Decreto Legislativo 70/2003

Reg. UE / 679/2019 noto come Regolamento Generale sulla Protezione dei Dati (GDPR);

Decreto legislativo n. 196/2003, integrato con il Decreto Legislativo n. 101/2010;

Legge 31 luglio 2005, n. 55 "Conversione in legge, con modifiche, del Decreto Legge del 27 luglio 2005, n. 144, contenente misure urgenti per combattere il terrorismo internazionale ", nella Gazzetta Ufficiale n. 177 del 1° agosto 2005;

Codice Penale italiano.

Codice di autoregolamentazione per i servizi Internet

Decreto Legislativo del 10 agosto 2018, n.101.

Decreto Legislativo del 30 giugno 2003, n.196;

Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica pubblicate ai sensi dell'Article 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 29 novembre 2018 [9067692];

Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali**,** Legge 675/1996;

Codice Civile Italiano.

Decreto Legislativo No. 70/2003 (implementing Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market), accessed 12 February 2020.

Decreto Legislativo n.70/2003

Decreto Legislativo 31 Luglio 2005, n. 177 (Testo Unico dei servizi di media audiovisivi e radiofonici), disponibile *online* al sito:
<https://www.camera.it/parlam/leggi/deleghe/testi/05177dl.htm>.

Costituzione Italiana 1948

Codice Penale Italiano 1930.

Reports

Lotta contro il terrorismo online: il Forum Internet dell'UE si impegna a rispettare un protocollo di crisi a livello dell'UE, Bruxelles, 7 ottobre 2019.

V. Azzolina, Chi ha paura della libertà di internet?, Torino, 2019.

Relazione Finale della Commissione "Jo Cox" sull'Intolleranza, la Xenofobia, il Razzismo e i Fenomeni di Odio, approvata nella seduta del 6 luglio 2017, disponibile *online* al sito:
<https://www.camera.it/application/xmanager/projects/leg17/attachments/uploadfile_commissione_intolleranza/files/000/000/001/RELAZIONE_FINALE.pdf>,
ultimo accesso in data 28 Gennaio 2020.

M.Orofino, "Article21 Cost: le ragioni per un intervento di manutenzione ordinaria" (2008)

P.Barile, "Diritti dell'uomo e libertà fondamentali" (1984)

F. Donati "L'art 21 della Costituzione 70 anni dopo" (2018)

C. Alvisi, *La protezione dell'Agcom degli interessi contrapposti ai titolari,* in AIDA 2014, 163.

M.C. Amorosi, *Terrorismo, diritto alla sicurezza e diritti di libertà: una riflessione intorno al decreto legge n. 7 del 2015,* in *Costituzionalismo,* fasc. 2, 2015

L. V. Berruti, *Blacklist e blocco dei contenuti web illeciti: dal contrasto alla pedopornografia al cyber terrorism. Commento al d.l. 7/2015, Article 2,* in *Legislazione penale,* 15.01.2016.

R. Bocchini, *Le nuove disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*, in *Nuove leggi civili commentate,* 2018, 340.

F. Goisis, *Profili di legittimità nazionale e convenzionale europea della repressione in via amministrativa delle violazioni del diritto d'autore sulle reti di comunicazione elettronica: il problema dell'enforcement,* in AIDA 2014, 180.

F. Piraino, *Spunti per una rilettura della disciplina giuridica degli internet service provider,* in AIDA 2017, 468.

P. Pittaro, *La legge sul cyberbullismo,* in *Famiglia e diritto,* 2017, 819.

M. Renna, *Le questioni di legittimità del regolamento dell'AGCOM sulla tutela del diritto d'autore online,* in AIDA 2014, 111.

Books

F. Di Ciommo, Diritto alla cancellazione, diritto di limitazione del trattamento e diritto all'oblio, in I dati personali nel diritto europeo, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Giappichelli Editore, Torino, 2019.

S. Rodotà, Il mondo nella rete. Quali i diritti, quali i vincoli, Editori Laterza, Roma, 2014.

F. Bassan, E. Tosi (Eds.), Diritto degli audiovisivi (Giuffrè, 2012).

M. Faccioli, *Minori nella rete. Pedofilia, pedopornografia, deep web, social network, sexting, gambling, grooming e cyberbullismo nell'era digitale* (Key Editore, 2015).

L.C. Ubertazzi (ed.), *Il Regolamento AGCOM sul diritto d'autore* (Giappichelli, 2014).

G. Ziccardi, *L'odio online* (Raffaello Cortina, 2016).

Periodicals

Pietro Maria Sabella, "Il fenomeno del *cybercrime* nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali", (2017), Informatica e diritto, 43 annata, vol. 26, page 171.

G. Pitruzella, La libertà di informazione nell'era di Internet, in Media Laws, Milano, 2018

O. Pollicino, La prospettiva costituzionale sulla libertà di espressione nell'era di Internet, in Media Laws, Milano, 2018

R. Pardolesi, L'ombra del tempo e (il diritto al)l'oblio, in Questione di Giustizia, Quarterly Journal, 1/2017.

Digital resources

https://www.roedl.it/it/attualita/legal-tech/la-responsabilit%C3%A0-degli-internet-service-provider/la-responsabilita-degli-internet-service-provider

https://www.altalex.com/documents/news/2019/03/20/diritto-d-autore-responsabilita-dell-hosting-provider

https://www.aiip.it/codice-autoregolamentazione-servizi-internet/

<http://www.diritto24.ilsole24ore.com/civile/civile/primiPiani/2013/07/internet-e-diritto-alloblio-una-recente-sentenza-del-tribunale-di-milano.php>

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3541955

http://www.dirittodellinformatica.it/ict/crimini-informatici/profili-legali-delle-fake-news.html.

Case law

Sezione specializzata per la Proprietà Intellettuale del Tribunale Civile di Roma, sulla richiesta di misure precauzionali proposta da FAPAV, Federazione Audiovisiva Anti-pirateria contro Telecom Italia;

Corte di Cassazione, sezione V pen., 19 luglio 2016, n. 6061;

Corte di Cassazione, Divisione Penale., Sezione V, 16 ottobre 2012, n. 44980; Corte di Cassazione, Divisione Penale, sezione V, 17 novembre 2000, n. 4741;

Corte di Cassazione n. 5525/2012.

Corte di Cassazione, sent. no. 31022/2015.

Cons. St., sez. VI, 15 luglio 2019, n. provvedimento 201904993.

Corte Costituzionale, sent. 1969 n.84

Corte Costituzionale, sent. 1962 n. 9

Sentenze della Corte di Cassazione:

16111/2013;

13161/2016;

38747/2017;

28084/2018;

19681/2019.

ELSA Lithuania

Contributors

National Coordinator

Andra Mažrimaitė

National Researchers

Deimantė Rimkutė

Vytautas Pasvenskas

Kristijonas Povylius

Milda Žaliauskaitė

National Academic Supervisor

Prof. dr. Vytautas Mizaras

Acknowledgements

Research group of ELSA Lithuania would like to express greatest appreciation for prof. dr. Vytautas Mizaras who kindly invested his time and effort in order to give us his constructive comments, valuable suggestions and guidelines that have helped us to shape and complete this report.

Introduction

Freedom of expression is one of the most important human rights. As the Universal Declaration of Human Rights states 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.'[1270] In fact, freedom of expression is protected under the national and international laws in Lithuania. Although this right grants an ability to express one's beliefs, opinions and ideas freely without unlawful censorship, it also conditions a duty to do it responsibly while also respecting other people's rights. And in the age of globalisation and information technologies where the internet has enabled new models of interaction, effective and respectful implementation and protection of freedom of expression has certainly become quite a complex matter. Therefore, this report analyses the main questions concerning internet censorship from Lithuania's legal system perspective.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

The Republic of Lithuania ensures and protects Freedom of Expression as one of the fundamental foundations and values of democratic society. This freedom, though valid with restrictions, is enshrined in several laws: primarily, in the Constitution of the Republic of Lithuania, also in the Criminal Code and the Law on the Provision of Information to the Public.

To begin with, freedom of expression is granted by the Constitution of the Republic of Lithuania. In particular, Article 25, which is rather lengthy and comprehensive, is mostly aimed at ensuring the right for everyone to have their

[1270] United Nations General Assembly, 'The Universal Declaration of Human Rights' <https://www.un.org/en/universal-declaration-human-rights/>.

own convictions and freely express them, i.e. (including seeking, receiving or imparting information and ideas), which '[f]reedom to express convictions, to receive and impart information may not be limited otherwise than by law when this is necessary to protect human health, honour or dignity, private life, or morals, or to defend the constitutional order'.[1271] Moreover, this Article clearly states the right to seek, receive and impart information freely. Accordingly, this fundamental principle was entrenched into various legal acts demonstrating its significance and necessity for protection.

The Criminal Code of the Republic of Lithuania is one of the main laws ensuring Freedom of Expression is exercised properly. There are certain safeguards in place aimed to limit abusive, improper, hence illegal, expression. For example, Article 154 establishes liability for two kinds of libel: for spreading 'false information about another person that could arouse contempt for this person or humiliate him or undermine trust in him'; and for libelling another person by 'accusing him of commission of a serious or grave crime or in the media or in a publication'.[1272] According to the Article 198, it is also unlawful to distribute or otherwise use the electronic data which may not be made public.[1273] It is necessary to mention Article 170, which states that a person or a legal entity may be held liable for such activities as: 1) distributing, producing, acquiring, sending, transporting or storing the items for the purposes of distribution that ridicules, expresses the contempt for, urges hatred of or incites discrimination; 2) publicly ridiculing, expressing contempt for, urging hatred of or inciting discrimination; 3) publicly inciting violence or a physical violent treatment, or financing or otherwise supporting such activities.[1274] These activities should be based on the grounds of sex, sexual orientation, race, nationality, language, descent, social status, religion, convictions or views and shall be punished by fine, restriction of liberty, arrest or by custodial sentence for a term of up to three years depending on the severity of activity.[1275] This statutory provision directly correlates with the Constitution as Article 25 of the latter one states that freedom to express convictions and to impart information is incompatible with criminal actions,

1271 The Constitution of the Republic of Lithuania, Article 25 <https://www.lrs.lt/home/Konstitucija/Constitution.htm>.

1272 The Criminal Code of the Republic of Lithuania, Article 154 <https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=q8i88l10w&documentId=a84fa232877611e5bca4ce385a9b7048&category=TAD>.

1273 The Criminal Code of the Republic of Lithuania, Article 198 <https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=q8i88l10w&documentId=a84fa232877611e5bca4ce385a9b7048&category=TAD>.

1274 The Criminal Code of the Republic of Lithuania, Article 170 <https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=q8i88l10w&documentId=a84fa232877611e5bca4ce385a9b7048&category=TAD>.

1275 ibid.

such as 'incitement to national, racial, religious, or social hatred, incitement to violence or to discrimination, as well as defamation and disinformation'.[1276] Herewith, Article 1.137 of the Civil Code of the Republic of Lithuania ensures freedom of enjoyment and exercise of civil rights, however, abuse of those rights is forbidden 'there being no legal ground, no civil rights may be exercised in a manner or by means intended to violate other persons' rights and interests protected by laws; or to restrict other persons in their rights and interests protected by laws; or with the intent of doing damage to other persons; or where this would be contrary to the purpose of the subjective right'.[1277]

With regards to legislation that protects against limitation towards freedom of expression, the Law on the Provision of Information to the Public is the principal law governing freedom of information. In its scope, this law is not limited only to electronic information, rather it encompasses all information. Mainly, this law grants and protects the right to freely express ideas and convictions and to collect, obtain and disseminate information and ideas.[1278] Similar to the Constitution and Criminal Code, this law states that freedom of information may be restricted only when two conditions are met: 1) restriction may be implemented only under the law; 2) restriction is allowed only in cases where it is necessary to protect the constitutional system, a person's health, honour, dignity, private life and morality[1279]. In addition to this, this law expressly states any form of censorship is prohibited in the Republic of Lithuania. In particular, Article 7 states that 'it shall be prohibited to exert pressure on the producer or disseminator of public information, their participant or a journalist, compelling them to present information in the media in an incorrect and biased manner' and Article 10 '[a]ny actions whereby an attempt is made to control the content of information to be published in the media before its publication, with the exception of cases provided for by law, shall be prohibited'.[1280] It is worth to mention, that the term 'censorship' is neither defined by the Law on the Provision of Information to the Public nor by other laws in Lithuania.

1276 The Constitution of the Republic of Lithuania, Article 25 <https://www.lrs.lt/home/Konstitucija/Constitution.htm>.

1277 The Civil Code of the Republic of Lithuania, Article 1.137 <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495>.

1278 Law on the Provision of Information to the Public, Article 4 <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2865241206f511e687e0fbad81d55a7c?jfwid=1clcwosx33>.

1279 ibid.

1280 Law on the Provision of Information to the Public, Article 7, 10 <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2865241206f511e687e0fbad81d55a7c?jfwid=1clcwosx33>.

Lastly, Freedom of Expression is protected as well as restricted by the courts of Lithuania. The Constitutional Court in its ruling of 13 February 1997 has stated that Freedom of Expression may be limited only under the law, when it is necessary for democratic society and such limitations should be assessed with regards to the criteria of common sense and evident necessity, also it is necessary to determine aim of limitation and ascertain whether limitation is proportionate to the relevant aim[1281]. In addition to this, the Constitutional Court has ruled that 'any limitation on the freedom of expression and information must always be conceived as a measure of exceptional nature'.[1282] As a matter of fact, freedom of expression is considered applicable not only to information or ideas 'that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness without which there is no 'democratic society'.[1283] It is evident that effective protection of freedom of expression is inseparable from balancing different interests and rights.

To sum up, laws of the Republic of Lithuania ensure and protect Freedom of Expression, however, this Right is not absolute. Freedom of Expression may be restricted only under the law and only in order to protect the constitutional system and other person's constitutional rights.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

Currently, Lithuania has several laws that regulate harmful content and sensitive information:

- Law on Public Information;
- Law on the Protection of Minors against the Detrimental Effects of Public Information;
- Law on Electronic Communications;
- Law on Information Society Services;
- Law on Copyright and Related Rights;
- Law on Gambling;
- Law on Consumer Rights Protection;

1281 The Constitutional Court ruling of 13 February 1997 <https://hudoc.echr.coe.int/eng#{"itemid":["001-180506"]}>.

1282 The Constitutional Court ruling of 10 March 1998 <https://hudoc.echr.coe.int/eng#{"itemid":["001-180506"]}>.

1283 European Court of Human Rights case of *Sekmadienis Ltd. v. Lithuania* of 30 January 2018 <https://hudoc.echr.coe.int/eng#{"itemid":["001-180506"]}>.

— Law on Alcohol control;
— And others.

2.1. Law on Public Information

One of the most important legal sources is Law on Public Information. Its Article 19 regulates the definition of sensitive information that is prohibited from publishing on the internet and has to be taken down. Information cannot be published if it:

— Encourages the violation of the sovereignty of Lithuania to change its constitutional order, independence or integrity of the territory;
— Promotes or initiates acts of terrorism;
— Propagates war propaganda, incitement to war or hatred, bullying, stigmatisation, incitement to discrimination, violence, physical abuse of a group or person based on age, gender, sexual orientation, ethnicity, race, nationality, citizenship, language, origin, social status, disability, religion, beliefs, beliefs, or religion;
— Distributes or promotes pornography, sexual services, sexual perversion;
— Promotes harmful habits and narcotic or psychotropic substances;
— Spreads disseminate misinformation and information that is defamatory, offensive, defamatory or degrading;
— Violates the presumption of innocence.

A person who considers that the creator or the publisher has potentially published sensitive information, has the Right to apply to the authority (Commission of Lithuanian radio and television) responsible for controlling sensitive information with a reasoned request for investigation, decision and imposition of objectively necessary measures. Such an authority is responsible for the control of sensitive information needed to examine the circumstances within 20 working days and take a decision. When the decision is taken, a person may appeal against the decision and complain to the Vilnius Regional Administrative Court.

Prosecutor or certain associations that have reason to believe that the authorities responsible for the control of sensitive information have not fulfilled or have failed to fulfil their statutory obligations in relation to the control of sensitive information. If such acts are contrary to the public interest, they can apply to the authority where the offense was committed with a reasoned request for the necessary steps to be taken to remedy the breach. If authority responsible for the control of sensitive information does not fulfil its duties within 20 working

days, the prosecutor or associations acting in the public information field shall have the right to apply to the Vilnius Regional Administrative Court as well.

If police become aware that the sensitive information referred to in the previous paragraphs has been disseminated on the internet should notify the providers of electronic information hosting services of the information. If electronic information hosting providers do not voluntarily remove or remove access to the information within two hours of receiving the notification, the police has a right to give the motivated mandatory instructions to the electronic information hosting service providers in order to restrict access to it for a maximum of 72 hours and longer if the Vilnius Regional Administrative Court approves. It also has a right to inform the Lithuanian Radio and Television Commission or the Inspector of Journalist Ethics about the issues.

In 2004, Government of Lithuania published Decision on the 'Approval of the Procedure for the Control of the Disclosure of Publicly Available Computer Networks and the Restriction of the Distribution of Public Information'. This document regulates the definition of 'Electronic media'. It is written that 'Electronic media' means websites of the media (press, television, radio) which convey public information in electronic form, disseminated in the usual manner, whether or not all or part of the content is transferred to the website. Mass media must be created in accordance with the procedure prescribed by laws by other natural and legal persons who wish to carry out or actually carry out mass media activities on public computer networks. Websites of public authorities and bodies for the distribution of official documents and information concerning the work of a public authority is not considered as electronic media.

2.2. Law on the Protection of Minor against the Detrimental Effects of Public Information

Another important legal source is Law on the Protection of Minor against the Detrimental Effects of Public Information. Article 4 regulates public information that adversely affects the development of minors. According to it, information which has a negative impact on minors is considered to be public information which may be harmful to the mental or physical health, physical, mental, spiritual or moral development of minors. The following is considered public information:

- Violent, promotes aggression and disrespect for life;
- Shows destruction or encourages destruction of property;
- Shows body of a deceased, dying or seriously injured person, except where such identification is required for identification purposes;

- Erotic;
- Causing fear or horror;
- Encourages gambling and other games with the impression of easy winning
- Favours and encourages the consumption, production, distribution or purchase of narcotic, toxic, psychotropic substances, tobacco or alcohol, as well as other substances used or likely to be used for intoxicating purposes;
- Promoting self-harm or suicide, detailing the means and circumstances of suicide;
- Which positively assesses the criminal act or idealises the criminals;
- Related to the modelling of a criminal offense;
- Promotes humiliating treatment;
- Defames or belittles a person or group of people on grounds of nationality, race, sex, origin, disability, sexual orientation, language, religion, beliefs, beliefs, or the like;
- When staged paranormal phenomena are displayed, giving the impression of its reality;
- Which promotes sexual abuse and exploitation of minors and sexual relations between minors;
- Which promotes sexual relations;
- Defamation of family values, promotion of a different concept of marriage and family formation than established in the Constitution of the Republic of Lithuania and the Civil Code of the Republic of Lithuania;
- Using obscene expressions, words or obscene gestures;
- Advising on the manufacture, purchase or use of explosives, narcotic drugs or psychotropic substances, as well as other life or health hazards;
- Promote poor diet, hygiene and physical inactivity;
- Mass hypnosis sessions targeted to a media audience.

However, rules set down in Article 4 have exceptions. For instance, as it is written in Article 5 information which has a negative impact on minors may be disseminated if its content consists only of information about events, political, social, religious or world views, the information is of scientific or artistic significance or is needed for research, education or education, it is in the public interest to publish it, its magnitude and impact are insignificant.

In almost all the cases, the dissemination of information that adversely affects minors shall be prohibited or restricted in accordance with the procedure

established by this Law. For example, the direct dissemination of information adversely affecting minors, such as offering, transferring or otherwise allowing it to be used personally, shall be prohibited. Such public information may be published only in places which are not accessible to minors and/or at times when minors cannot access it (for example, during the night), or where technical means enable persons responsible for the education and care of children to restrict the supply of such public information. for minors. The dissemination of information such as defames or belittles a person or group of people on grounds of nationality, race, sex, origin, disability, sexual orientation, language, religion, beliefs, beliefs, or the like is prohibited by law, in particular pornographic content, as well as information that promotes the sexual abuse and exploitation of minors and/or presents intentional violence.

2.3. Law of the Republic of Lithuania on Information Society Services

Another regulation aiming to set the rules to the provision of information society services and other activities of information society service providers is the Law of the Republic of Lithuania on Information Society Services, that implements EU Directive 2000/31. This law in its Article 4(3) delegates rights to competent public authorities (in this case - Information Society Development Committee) to go to the court and seek for needed measures that restrict the freedom to provide information services to the public and for prescribing their validity in Lithuania.

The rules set down in the Law of the Republic of Lithuania on Information Society Services are also applied to EU players and regulates restriction of information that is coming from the member states in exceptional situations. In such cases, two conditions, that are found in Article 4(3)(2-3), must be fulfilled. Firstly, legal grounds for restrictions are quite general and need to be associated with the prevention of the public interest, investigators, the discovery and formation of persons experiencing hardship, gender, religious or national hate speech, including personalities or individuals living in private, public security, national security and defence, interests, consumers, including investors, protection. Secondly, the competent authority (Information Society Development Committee) before going to the court, must address institutions in the member state, where the service provider is established, with a request that the competent authority take such measures, or considers that the measures are inadequate, the provider is established, of the intention of the competent authority to apply to the courts or the power to take action. As it is found in Article 4(4), the situations with an urgent matter with the EU condition are treated differently. Provision of information could be restricted without the

decision of the court. In cases like this, the competent authority without a delay needs to inform the European Commission and the member state of EU, where the service provider is established.

Moreover, in the Law on Information Society Services Article 15 obliges server providers to immediately inform the authority of any alleged unlawful activity of the recipient of the service or that the information supplied by the recipient may be obtained, created or altered in an unlawful manner. These providers should also provide all the information enabling the recipients of the services to be identified with whom the service providers have agreed to store information.

2.4. Law on Copyright and Related Rights

Law on Copyright and Related Rights[1284] (hereinafter the Law) defines implementation, administration and defence of copyrights and related rights. One of the remedies for defence of copyrights is a right by defendants of copyrights to apply for an injunction against an intermediary, with the aim of prohibiting him from rendering services in a network to third parties who make use of these services infringing a copyright, related right or sui generis right. This procedure is defined in Article 78 in LCRR in detail.

Two different procedures are enshrined in the Law – general and special. They have differences regarding subjects, authorities involved, scope of legal grounds and legal remedies.

2.4.1. General procedure

This procedure may be used in case of infringement of copyrights in general occurs. Only owners of copyright, related rights and sui generis rights may use this remedy. They have a right to apply for an injunction against an intermediary, with the aim of prohibiting him from rendering services in a network to third parties who make use of these services infringing a copyright, related right or sui generis right. An injunction to render the said services shall encompass suspension of a transmission of information related to the infringement of copyright, related rights or sui generis rights or elimination of such information, if an intermediary have technical means to carry this out, or removal of the access to information infringing copyright, related rights or *sui generis* rights.

2.4.2. Special procedure

This procedure is created for a special purpose – to fight against unlawful publication of copyrighted content in the internet. Therefore, it is the only legal

[1284] The Law on Copyrights and Related Rights of the Republic of Lithuania, No VIII-1185, approved on 18 May 1999.

ground on which this legal remedy may be applied. This procedure is simpler and more operative for defenders of copyrights than judicial procedure. Worth mentioning that this procedure is not mandatory for subjects who enjoy the right to defend copyrights, related rights and sui generis rights. They may use general procedure as well.

Special procedure has a wider range of subjects than general one. Apart from owners of copyright, related rights and *sui generis rights*, entities authorised by them and collective copyright management association may be subjects to this remedy as well.

The essence of this procedure is that defenders of copyrights, related rights and *sui generis* rights no longer need to sue infringers in a court in order to shut them down. It saves plenty of time and money for these subjects. Besides courts, special procedure involves additional authority – The Radio and Television Commission of Lithuania (hereinafter the Commission). The Commission has a right to give compulsory orders for internet services providers to remove access to a content which was made public unlawfully by blocking internet domain name that identifies a website as long as an infringement of copyrighted content is not removed. Before implementation of these orders, they shall be sanctioned by Vilnius Regional Administrative Court.

2.5. Law on Gambling

According to Article 20-7 of Law on Gambling,[1285] Game Control Authority, which is responsible for control of gambling market in Lithuania, has a right to give a compulsory order for network service providers to remove an access to information, which is used for organising remote illegal gambling.

2.6. Law on Consumer Protection

According to Article 49-1 of Law on Consumer Protection,[1286] State Consumer Rights Authority has a right to give a compulsory order for network service providers, also for other service providers which uses these services, to remove an access to information by blocking website's domain name until infringements of consumers' rights cease to exist.

[1285] The Law on Gambling of the Republic of Lithuania, No IX-325, approved on 23 May 2001.
[1286] The Law on Consumer Protection of the Republic of Lithuania, No I-657, approved on 7 December 1994.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

Lithuania has different legal grounds and conditions upon which content must either be blocked or taken down. These categories fall under criminal law or other laws and should be treated differently, therefore it aims to regulate different values and has different measures.

3.1. Criminal Law

One of the values that is being protected under the Criminal Code[1287] is national security, related to national independence, territorial integrity and constitutional order. Criminal Code prohibits crimes such as espionage (Article 119), public incitement to violate the sovereignty of the Republic of Lithuania with violence (Article 122), Unlawful disposal of information which is a state secret (Article 124), exposure (Article 125) or loss (Article 126) of state's secret.

Another value is the honour and dignity. The only crime (or misdemeanour) that violates honour and dignity of a person is defamation (Article 154). Defamation in the context of criminal code should be separated from the other rights related to the protection or reputation, that are regulated under the civil code. Criminal Code also protects the right to private life - unauthorised disclosure or use of a person's privacy (Article 168). Information about another person's private life that is publicly disclosed, used for the benefit of others is treated as a crime (or misdemeanour) if it was collected in an illegal way. Values of public morals and health in the Criminal Code are linked with the section of Crimes and misdemeanours to children and families. One of the crimes is Child abuse for pornography (Article 162), Possession of pornographic content (Article 309).

Another group of crimes and misdemeanours belong to the section of equality and freedom of conscience virtues. Under this category fall the illegal activities such as discrimination on the grounds of nationality, race, sex, origin, religion or other group affiliation (Article 169), incitement against any group of people of any nationality, race, ethnicity, religion or otherwise (Article 170), public acceptance, denial or gross denial of international crimes, crimes committed by the USSR or Nazi Germany against the Republic of Lithuania or its residents (Article 170-2), interference with religious ceremonies or celebrations (Article 171).

Protection of intellectual and industrial property rights is also included in the Criminal Code. The misappropriation of authorship (Article 191), Unauthorised

[1287] The Criminal Code of the Republic of Lithuania, No VIII-1864, approved on 25 October 2000.

reproduction, distribution, transportation or storage of unauthorised copies of a literary, scientific, artistic or related object (Article 192), Deletion or alteration of copyright or related rights management information (Article 193), Unauthorised removal of technical protection measures for copyright or related rights (Article 194), Infringement of Industrial Property Rights (Article 195). Crimes and misdemeanours to economy and business practice is also included in the Criminal Code such as Disclosure of commercial secrets (Article 211).

3.2. Civil Law

Civil Code of the Republic of Lithuania[1288] (hereinafter Civil Code) has several Articles which are important in the context of internet censorship: Article 2.22 (Right to an Image), Article 2.23 (Right to Privacy and Security), Article 2.24 (Protection of Honour and Dignity).

Civil Code protects Right to an Image. Protection of this Right is important, *inter alia*, for subjects who publish photographs or other images in the internet. According to Article 2.22 of Civil Code, Photograph (or its part) or some other image of a natural person may be reproduced, sold, demonstrated, published and the person may be photographed only with his consent. Natural person whose right to image has been infringed enjoys the right to request the court to oblige the discontinuance of the said acts and redressing of the property and non-pecuniary damage.

Article 2.23 of Civil Code aims to protect Right to Privacy and Security. According to this Article, Information on person's private life may be made public only with his consent. Dissemination of the collected information on the person's private life shall be prohibited unless, taking into consideration person's official post and his status in the society, dissemination of the said information is in line with the lawful and well-grounded public interest to be aware of the said information. Public announcement of facts of private life, however truthful they may be, as well as making private correspondence public in violation of the procedure prescribed in the given Article shall form the basis for bringing an action for repairing the property and non-pecuniary damage incurred by the said acts.

Article 2.24 of Civil Code protects honour and dignity. This Article grants the right for courts to make subjects of mass media to refute a published content. According to this Article, a person shall have the Right to demand refutation in judicial proceedings of the publicised data, which abase his honour and dignity, and which are erroneous. Where erroneous data were publicised by a mass

[1288] The Civil Code of the Republic of Lithuania, No VIII-1864, approved on 18 July 2000.

medium (press, television, radio etc.) the person about whom the data was publicised shall have the right to file a refutation and demand the given mass medium to publish the said refutation free of charge or make it public in some other way. Where a mass medium refuses to publish the refutation or make it public in some other way or fails to do it in the term set by the law, the person gains the Right to apply to court. The court shall establish the procedure and the term for the refutation of the data, which were erroneous or abased another person's reputation. Where the court judgement, which obliges the refutation of erroneous data abasing person's honour and dignity, is not executed, the court may issue an order to recover a fine from the defendant for each day of default.

3.3. Public Laws

Public laws such as Law on Public Information, Law on the Protection of Minor against the Detrimental Effects of Public Information, Law on Copyright and Related Rights, Law on Gambling, Law on Consumer Protection have various values listed which are protected by various legal remedies. One of those legal remedies – taking down or blocking the content which may cause damage to those values. There are two types of values: general and special. General values are protected no matter to whom content which infringes those values is addressed. Meanwhile, special values are protected in case a content is addressed or accessible to certain groups of the society (for example, minors).

3.3.1. General grounds

General grounds are listed in the Law on Public Information, Law on Gambling and in the Law on Copyrights and Related Rights. Those grounds could be divided into 8 categories:

- National Security (encouragement of the violation of the sovereignty of Lithuania to change its constitutional order, independence or integrity of the territory; war propaganda; incitement of war (Law on Public Information Article 15)).
- Psychical or psychological aggression (promotion or initiation acts of terrorism; incitement of hatred, bullying, stigmatisation; incitement of discrimination, violence, physical abuse of a group or person based on age, gender, sexual orientation, ethnicity, race, nationality, citizenship, language, origin, social status, disability, religion, beliefs, beliefs, or religion (Law on Public Information Article 15)).
- Sexual images and information (distribution or promotion pornography, sexual services, sexual perversion (Law on Public Information Article 15)).

- Harmful habits (promotion of harmful habits and narcotic or psychotropic substances (Law on Public Information Article 15)).
- Misinformation (spread of disseminate misinformation and information that is defamatory, offensive, defamatory or degrading (Law on Public Information Article 15))
- Judicial (violation of the presumption of innocence (Law on Public Information Article 15))
- Harm to property (infringement of copyrights and related rights (Law on Copyright and Related Rights Article 78)).
- Illegal economic activities (remote illegal gambling (Law on Gambling Article 20-7). economic activities which infringe rights of consumers (Law on Consumer Protection Article 49-1)).

3.3.2. Special grounds

Apart from general grounds, there are special grounds on which internet content may be blocked or taken down. In order to use this legal remedy under special grounds, one additional clause shall be fulfilled – information which causes violation shall be addressed or accessible to minors (people under age 18). There are 11 types of information listed in Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4:

- Psychical or psychological aggression directed either towards the self or towards the others (promotion of violence, aggression and disrespect for life; promotion of information causing fear or horror; promotion of self-harm or suicide, detailing the means and circumstances of suicide; humiliating treatment; defamation and belittling of a person or group of people on grounds of nationality, race, sex, origin, disability, sexual orientation, language, religion, beliefs, beliefs, or the like).
- Destruction of property (showing of destruction or promoting destruction of property).
- Cruel images (showing body of a deceased, dying or seriously injured person, except where such identification is required for identification purposes).
- Sexual images and information (showing erotic; promotion of sexual abuse and exploitation of minors and sexual relations between minors; promotion of sexual relations).
- Psychical or mental health (promotion of poor diet, hygiene and physical inactivity).
- Harmful habits (promotion of consumption, production, distribution or purchase of narcotic, toxic, psychotropic substances, tobacco or alcohol,

as well as other substances used or likely to be used for intoxicating purposes).
- Criminal (idealisation or positive representation of criminals or criminal acts; modeling of criminal offence).
- Moral grounds (defamation of family values, promotion of a different concept of marriage and family formation than established in the Constitution of the Republic of Lithuania and the Civil Code of the Republic of Lithuania; using obscene expressions, words or obscene gestures).
- Misinformation (display of staged paranormal phenomena, giving the impression of its reality).
- Advises on the manufacturing of dangerous hazards (advising on the manufacture, purchase or use of explosives, narcotic drugs or psychotropic substances, as well as other life or health hazards).
- Psychological effect (mass hypnosis sessions targeted to a media audience).

3.4. Relationship between criminal and other laws

Some of values which could be infringed in the internet space, are protected only by civil and public laws, but some of them are also protected by criminal laws. It probably suggests that values which are the most important are protected by both other and criminal laws. Not every value needs to be protected by criminal laws. This paragraph will examine which of the values are protected only by other laws, and which values are protected by both other and criminal laws.

3.4.1. Values protected by both criminal and other laws

This paragraph will list values which are protected by both criminal and other laws: National security, honour and dignity, equality and freedom of conscience virtues, intellectual and industrial property rights.

- National security
    - Criminal Code:

i. Espionage (Article 119)

ii. Public incitement to violate the sovereignty of the Republic of Lithuania with violence (Article 122)

iii. Unlawful disposal of information which is a state secret (Article 124)

iv. Exposure (Article 125) or loss (Article 126) of state's secret

- Other laws:

  Encouragement of the violation of the sovereignty of Lithuania to change its constitutional order, independence or integrity of the territory; war propaganda; incitement of war (Law on Public Information Article 15).

— Honour and dignity
  - Criminal Code:

    Defamation (Article 154).

    Unauthorised disclosure or use of a person's privacy (Article 168).

    Child abuse for pornography (Article 162).

    Possession of pornographic content (Article 309).

  - Other laws:

    Right to an image (Civil Code Article 2.22).

    Right to privacy and security (Civil Code Article 2.23).

    Honour and dignity (Civil Code Article 2.24).

    Showing erotic; promotion of sexual abuse and exploitation of minors and sexual relations between minors; promotion of sexual relations (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

v. Distribution or promotion pornography, sexual services, sexual perversion (Law on Public Information Article 15).

— Equality and freedom of conscience virtues
  - Criminal Code:

vi. Discrimination on the grounds of nationality, race, sex, origin, religion or other group affiliation (Article 169).

vii. Incitement against any group of people of any nationality, race, ethnicity, religion or otherwise (Article 170).

viii. Public acceptance, denial or gross denial of international crimes, crimes committed by the USSR or Nazi Germany against the Republic of Lithuania or its residents (Article 170-2).

ix. Interference with religious ceremonies or celebrations (Article 171).

- Other laws:

x. Promotion or initiation acts of terrorism; incitement of hatred, bullying, stigmatisation; incitement of discrimination, violence, physical abuse of a group or person based on age, gender, sexual orientation, ethnicity, race, nationality, citizenship, language, origin, social status, disability, religion, beliefs, beliefs, or religion (Law on Public Information Article 15).

Defamation and belittling of a person or group of people on grounds of nationality, race, sex, origin, disability, sexual orientation, language, religion, beliefs, beliefs, or the like (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

— Intellectual and industrial property rights
  - Criminal Code:

The misappropriation of authorship (Article 191).

Unauthorised reproduction, distribution, transportation or storage of unauthorised copies of a literary, scientific, artistic or related object (Article 192).

Deletion or alteration of copyright or related rights management information (Article 193).

Unauthorised removal of technical protection measures for copyright or related rights (Article 194).

Infringement of Industrial Property Rights (Article 195).

Disclosure of commercial secrets (Article 211).

  - Other laws:

Infringement of copyrights and related rights (Law on Copyright and Related Rights Article 78).

3.4.2. Values protected only by other laws

Such values as avoidance of harmful habits, correct information, presumption of innocence, restriction of illegal economical activities, avoidance of destruction of property, avoidance of cruel images, morality, avoidance of criminal behaviour, restriction of advises on the manufacturing of dangerous hazards, psychological condition.

— Avoidance of harmful habits

- Promotion of harmful habits and narcotic or psychotropic substances (Law on Public Information Article 15).
- Promotion of consumption, production, distribution or purchase of narcotic, toxic, psychotropic substances, tobacco or alcohol, as well as other substances used or likely to be used for intoxicating purposes (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

— Correct information
- Spread of disseminate misinformation and information that is defamatory, offensive, defamatory or degrading (Law on Public Information Article 15).
- Display of staged paranormal phenomena, giving the impression of its reality (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

— Judicial
- Violation of the presumption of innocence (Law on Public Information Article 15).

— Restriction of illegal economic activities
- Remote illegal gambling (Law on Gambling Article 20-7).
- Economic activities which infringe rights of consumers (Law on Consumer Protection Article 49-1).

— Avoidance of destruction of property
- Showing of destruction or promoting destruction of property (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

— Avoidance of cruel images
- Showing body of a deceased, dying or seriously injured person, except where such identification is required for identification purposes (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4)

— Avoidance of criminal behaviour
- Idealisation or positive representation of criminals or criminal acts; modelling of criminal offence (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

— Morality
- Defamation of family values, promotion of a different concept of marriage and family formation than established in the Constitution of the Republic of Lithuania and the Civil Code of

the Republic of Lithuania; using obscene expressions, words or obscene gestures (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

- Restriction of advises on the manufacturing of dangerous hazards
  - Advising on the manufacture, purchase or use of explosives, narcotic drugs or psychotropic substances, as well as other life or health hazards (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4)
- Psychological condition
  - Mass hypnosis sessions targeted to a media audience (Law on the Protection of Minor against the Detrimental Effects of Public Information Article 4).

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

Internet content regulation, including self-regulation, is a not one of the most popular topics of discussions in Lithuania. This topic still receives very little attention; therefore, this might be the primary reason for lack self-regulatory measures undertaken by the private sector.

With regards to legislation, internet content regulation is only available with legal measures, not that much with self-regulatory ones. To illustrate this, there are such laws as the Law on the Protection of Minors against the Detrimental Effect of Public Information, the Criminal Code, Code of Administrative Offenses, Procedure for control of disclosure and distribution of restricted public information on computer networks for public use adopted by the Government, that do state and describe sensitive information and information that is restricted to be published. For example, according to the Article 6 of the Law on the Protection of Minors against the Detrimental Effect of Public Information, '[i]t shall be prohibited to disseminate in the mass media information having a detrimental effect on minors related to personal data'.[1289] However, there are no codes of self-regulation or codes of ethics on self-regulation, at least the ones that are made public, adapted in Lithuania up to this day. Many private entities still believe they are not responsible for publishing information that is sensitive or prohibited from publishing.[1290] There were several initiatives to look for ways

[1289] Law on the Protection of Minors against the Detrimental Effect of Public Information, Article 6 <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.363137?jfwid=rivwzvpvg>.

[1290] Gudaitis, R., 'Žalingo turinio informacijos priežiūra elektroninėje žiniasklaidoje: reguliavimo problemos ir perspektyvos' <https://www.lrs.lt/apps3/1/2411_CQAXHHCZ.PDF>.

to promote internet content self-regulation (for example, a seminar organised by Information Society Development Committee under the Government of the Republic of Lithuania aimed to discuss such issues[1291] or the initiative to create common electronic marketing self-regulation code in 2004), however, these initiatives have not led to the effective results.

To summarise, internet content self-regulation by the private sector in Lithuania is rather secluded issue that does not receive sufficient attention. Private sector is not keen enough to regulate the content on self-regulatory basis, therefore, there must be some high quality measures adapted by the state in order not only to activate private sector to regulate internet content, but also to help them choose appropriate self-regulatory measures and achieve effectiveness.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

Firstly, Lithuania lawmakers copied personal data definition and the main data protection law rules form GDPR to Law on Legal Protection of Personal Data of the Republic of Lithuania. Article seven provides examples when person can demand to erase his/her data. For example, they are incorrect and do not contradict established data collection procedures; data collection is not allowed by individuals. Due to this, there are no noticeable differences in legal regulation.

In 2019, the State Data Protection Inspectorate had about seven percent complaints about processing personal data. Most frequent complaints were about the Right to be Forgotten and the Right to Access personal data. The same year, due to this violation of the Right to Access personal data and the Right to be Forgotten the municipality institution received a fine of two thousand three hundred and ninety-five euros. This decision was approved by Vilnius Regional Administrative Court.[1292]

However, in two years since the GDPR implementation in Lithuanian's national law system, courts did not receive a specific case about the right to be forgotten. The majority of cases were about access to personal data and collecting and processing personal data.

[1291] Internet content regulation issues discussed during the interactive seminar <https://ivpk.lrv.lt/lt/naujienos/interaktyvaus-seminaro-metu-aptarti-interneto-turinio-reguliavimo-klausimai-1>.

[1292] "Bendrasis duomenų apsaugos reglamentas. Ginama teisė susipažinti su savo asmens duomenimis", *Valstybinė duomenų apsaugos inspekcija*, 14 August 2019 <https://vdai.lrv.lt/lt/naujienos/bendrasis-duomenu-apsaugos-reglamentas-ginama-teise-susipazinti-su-savo-asmens-duomenimis>

6. How does your country regulate the liability of internet intermediaries?

In the Constitution of the Republic of Lithuania Article 25 is said that everyone shall have the right to have his own convictions and freely express them. However, the freedom to express convictions and to impart information shall be incompatible with criminal actions. Moreover, in Lithuanian Criminal Code Article 170 is said that Anyone who, for distribution, has produced, purchased, shipped, transported, held, used to discredit, denigrate, hating or inciting discrimination or has publicly ridiculed, despised, hated, or incited to discriminate against a group or person based on age, gender, sexual orientation, disability, race, nationality, language, origin, social status, beliefs.

When talking about the liability of internet intermediaries The Law on Information Society Services of the Republic of Lithuania is very important, because it implemented directives' 2000/31/EC Articles 12-14to Lithuanians National law.[1293]

This law gives insight to ground definitions of the internet the liability of internet intermediaries. For example, what is Commercial information, Competent Authority and Service Provider.

Moreover, on 1 April 2019 Lithuanian lawmakers changed the Law on Copyright and Related Rights, according to which the Lithuanian Radio and Television Commission will be able to decide, under an accelerated procedure, to block access to websites in the event of an infringement of copyright or related rights. Before this change, the procedure was that it was needed to get court permission. The blocking procedure was very slow and not efficient and it was necessary to make it more flexible and faster.[1294]

The most famous Lithuania case is about trying to shut down the most popular illegal torrent internet page called *Linkomanija*. 4 July 2019 Supreme Court of Lithuania decided that although circumvention of the linkomanija.net blocking tool exists, this does not mean that such a remedy for copyright and other intellectual property rights is inappropriate in terms of effectiveness.[1295]

[1293] The European Parliament and of the Council directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (2000) Official Journal L178, page 12-13 <000L0031&from=LT"https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri =CELEX:32000L0031&from=LT>.

[1294] Balčiūnienė, R. 'Kaip veiks neleistino turinio blokavimas internete', *Verslo žinios,* 1 April 2019 <https://www.vz.lt/rinkodara/2019/04/01/kaip-veiks-neleistino-turinio-blokavimasinternete>.

[1295] Supreme Court of Lithuania case No.: e3K-3-236-969/2019

Also, in 2019 Lithuanian Radio and Television Commission made the decision to block mirror sites of pages which shares illegal content.[1296] Mirror Site: A mirror site is a website that contains identical content to another website. This content is usually 'mirrored' in order to serve as a duplicate or backup of the original site's content. This decision was made in accordance with the Description of the Procedure for the Application of Mandatory Instructions to Internet Access Service Providers, approved by the Minister of Culture of the Republic of Lithuania on 25 November 2019 Order no. ĮV-771 Approval of the Description of the Procedure for the Application of Mandatory Instructions to Internet Access Providers. In general, In Lithuania obligation for blocking and taking down content exists for illegal pirated content.

So, in Lithuania freedom of expression in all forms is mainly protected by Constitution, but as long as it does not violate the rights of others i.e. freedom of expression and dissemination incompatible with criminal activity - incitement to hatred, slander and misinformation based on national, racial, religious or social hatred, violence or discrimination.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Most likely legislation, regarding online content blocking and take-down, liability of internet intermediaries and the Right to be Forgotten, will be applied more broadly and the list will expand. This premise is based on the new amendments of Law on Consumer Rights Protection and other laws.

Another argument could be based on technological innovations expansion, that are connected to online content. It is possible that new laws will emerge and regulate the market players.

Some laws such as Law on Public Information or Law on the Protection of Minors against the Detrimental Effects of Public Information have norms that possibly discriminate LGBT community, since they prohibit information related propagating LGBT. It is likely that new legislators with a more liberal attitude will eliminate these articles.

[1296] Keršienė, B. "LRTK įgaliota blokuoti veidrodines interneto svetaines, kuriose skelbiamas nelegalus turinys", ELTA, 4 December 2019, <https://www.elta.lt/lt/pranesimai-spaudai/lrtk-igaliota-blokuoti-veidrodines-interneto-svetaines-kuriose-skelbiamas-nelegalus-turinys-193820>.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

Lithuania has an issue with a hate speech in an online environment. In the cyberspace - Internet comments, social websites, approximately 90% of the acts of incitement to hatred are committed each year.[1297] Unfortunately, in most cases, law enforcement tends to not to start an investigation. A few possible reasons for that are: 1) officers' mentality is that online hate is not enough serious crime to undertake; 2) there are not enough resources to look into every hate speech case in an online environment; 3) only in recent years this issue got public attention.

In Lithuania, limitations of freedom of expression online are more focused on illegal content on the internet. National laws have stricter regulations on pirating online than on hate speech in internet comments. Only Constitution and Criminal Code[1298] say that all forms of intolerance, e.g. inciting violence comments on news portal or social media, for persons' race, sex, sexually is prohibited by law. However, in practices law enforcement is not giving sufficient attention to this type of crime. On the other hand, in recent years, the public started to give attention to hate which is happening on the internet, and due to this, police are forced to take action on these vicious comments.

It must be concluded that Lithuania has not reached an adequate balance between allowing freedom of expression online and protecting against hate speech in an online environment. Thus, Lithuania needs to start not only limiting pirating content ways but also tackle various offensive actions which are happening on cyberspace.

[1297] Kuktoraitė, E. 'Neapykantos kurstymas internete: žmogaus teisė į orumą – saviraiškos laisvės užribyje?' *ManoTeisės*, 2 February 2018 <https://manoteises.lt/straipsnis/neapykantos-kurstymas-internete-zmogaus-teise-i-oruma-saviraiskos-laisves-uzribyje/>.

[1298] The Criminal Code of the Republic of Lithuania, Article 170.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

Considering the legal framework regarding Freedom of Expression, it is evident that the laws properly promote and ensure firm protection of this right. However, it is also enshrined in laws that Freedom of Expression is not an absolute Right. It is allowed to enjoy and exercise this right, yet not at the expense of other rights, other people's rights and values. Freedom of expression may be limited in order to protect national security, constitutional order, other people's honour and dignity, intellectual and industrial property rights, etc. In addition to this, courts of Lithuania seek for proportionality and strikes for the right balance between Freedom of Expression and protection of other Rights. However, in practice there still remain certain challenges, mostly connected to the protection of other person's intellectual rights (piracy). Although Lithuania takes measures to fight piracy, yet this issue still needs more attention and more effective approaches.

10. How do you rank the access to freedom of expression online in your country?

Since Lithuania is a part of the Council of Europe and is under the control of European Court of Human Rights (hereinafter ECtHR), authors of this work presume that national laws regarding freedom of expression online are in the line with requirements which derive from the European Convention of Human Rights. As a result, those national laws will not be the object of this paragraph. However, proper laws do not always indicate a proper application of it. Lithuania and its judicial system is not an exception to this rule. There are several problems regarding the application of laws on freedom of expression online. This paragraph will examine whether Lithuanian laws on freedom of expression are interpreted by the local judicial system the same as it is interpreted by the ECtHR.

One of the problems widely discussed in public is hate speech in the internet against a particular group of people. Although this problem exists not only on the internet, but also elsewhere, the internet is a space where this problem is really striking, especially talking about social platforms or news portals and their sections for public comments. People in Lithuania still think that the section for comments on the internet is the place to express their opinion without any restrictions. The opinion exists that no one is liable for content which people

post in comment sections. It is one of the main challenges in Lithuania nowadays for both Lithuanian education and judicial systems – to educate people that the internet is the same public space as newspapers, shopping centres, city squares, etc. Therefore, the internet is a subject to the same restrictions as any other public space. No one shall publicly ridicule, express contempt for, urge hatred of or incite discrimination against a group of people or a person belonging thereto on the any grounds.

Recent case in the ECtHR *Beizaras and Levickas v. Lithuania* (no. 41288/15, 14 January 2020)[1299] is the outcome of this problem. Short outline of facts: one of the applicants posted a photograph on his Facebook page depicting a same-sex kiss between him and the other applicant. The picture was accessible not only to his Facebook 'friends', but also to the general public. The intention of posting the picture publicly was to announce the beginning of the applicants' relationship. The picture received many 'likes' and comments. Among comments were such as 'they should be castrated or burnt', 'If I was allowed to, I would shoot every single one of them', 'Scum!!!!!!! Into the gas chamber with the pair of them', 'Kill…' and similar. Couple days later both applicants lodged a written request with the LGL (acronym for Lithuanian Gay League) Association asking it to notify, in its own name, the Prosecutor General's Office of the hateful comments left under the photograph posted on the first applicant's page. According to the request, the comments quoted 'incited violence and physically violent treatment' and that such actions were criminal and merited pre-trial investigation. The complaint was lodged on the basis of Article 170 part 2 and part 3 of the Criminal Code ('Incitement against any national, racial, ethnic, religious or other group of people'). Three instances – prosecutor, district court and regional court – did not see an element of a crime under the Criminal Code. According to them, comments were 'unethical', but not criminal. Prosecutor and judges used arguments such as 'there was no systematic action', 'the authors of the comments had been merely expressing their opinion, instead of seeking to incite hatred or violence against individuals who were distinguishable by their sexual orientation', 'the authors of the impugned comments had chosen improper words to express their disapproval of homosexual people', etc. Since the decision by a regional court was final, the Applicants filed the application to ECtHR. The court decided that Lithuania infringed Article 13 (Right to an effective remedy) and Article 14 (Prohibition of discrimination) of European Convention of Human Rights because Lithuanian judicial authorities refused to initiate pre-trial investigation.

[1299] *Beizaras and Levickas v. Lithuania* (no. 41288/15, ECHR, 14 January 2020).

The case *Beizaras and Levickas v. Lithuania* is a symbol that not all people of Lithuanian society consider the internet as public space where the same restrictions as in any other traditional public space are applied. Moreover, sometimes even highly qualified officers in national judicial authorities do not always find that Freedom of Expression has its boundaries.

To sum everything up, access to Freedom of Expression online in Lithuania is high. However sometimes, when that freedom is used for ridicule, expression of contempt, urge of hatred, incitement of discrimination against other people, it should be restricted. We give 4.5 of 5 for the access to freedom of expression online in Lithuania.

11. How do you overall assess the legal situation in your country regarding internet censorship?

Overall, Lithuania is not the strictest country on internet censorship. Legal framework provides an ability to freely express one's mind, beliefs and ideas even if those are not favourably received or regarded, and that might potentially shock or disturb others. However, limitations come into force when freedom of expression violates other people's rights or endangers the constitutional system. Laws and courts while adapting laws seek for balance between competing freedoms and rights, and there still remains some issues in practice. Above all, Lithuania's legal system is in the positive direction and may be considered as a rather effective one in the EU.

Conclusion

Lithuania is a part of European Union and legal acts which are dedicated to freedom of expression online and in general freedom of speech. It must be concluded that Lithuania is a modern Western country. However, like in every country there are some issues regarding a balance between freedom and respect for the rights of others.

Table of legislation

Provision in Lithuanian language	**Corresponding translation in English**
LIETUVOS RESPUBLIKOS BAUDŽIAMASIS KODEKSAS	THE CRIMINAL CODE OF THE REPUBLIC OF LITHUANIA
119 straipsnis. Šnipinėjimas 1. Tas, kas turėdamas tikslą perduoti užsienio valstybei, jos organizacijai pagrobė, pirko ar kitaip rinko informaciją, kuri yra Lietuvos Respublikos valstybės paslaptis, arba šią informaciją perdavė užsienio valstybei, jos organizacijai ar jų atstovui, baudžiamas laisvės atėmimu nuo dvejų iki dešimties metų. 2. Tas, kas vykdydamas kitos valstybės ar jos organizacijos užduotį pagrobė, pirko ar kitaip rinko arba perdavė informaciją, kuri yra Lietuvos Respublikos valstybės paslaptis, arba kitą užsienio valstybės žvalgybą dominančią informaciją, baudžiamas laisvės atėmimu nuo trejų iki penkiolikos metų.	Article 119. Espionage 1. A person who, for the purpose of communicating it to a foreign state or organisation thereof, seizes, purchases or otherwise collects the information constituting a state secret of the Republic of Lithuania or communicates this information to a foreign state, organisation thereof or their representative shall be punished by a custodial sentence for a term of two up to ten years. 2. A person who, in performing an assignment of another state or organisation thereof, seizes, purchases or otherwise collects or communicates the information constituting a state secret of the Republic of Lithuania or another information of interest to the intelligence of a foreign state shall be punished by a custodial sentence for a term of three up to fifteen years.
122 straipsnis. Vieši raginimai smurtu pažeisti Lietuvos Respublikos suverenitetą Tas, kas viešai ragino smurtu pažeisti Lietuvos Respublikos suverenitetą – pakeisti jos konstitucinę santvarką, nuversti teisėtą valdžią, kėsintis į jos nepriklausomybę arba pažeisti teritorijos vientisumą, šiems tikslams kurti ginkluotas grupes arba daryti kitus šiame skyriuje numatytus nusikaltimus, kuriais kėsinamasi į Lietuvos valstybę, baudžiamas laisvės atėmimu iki penkerių metų.	Article 122. Public Incitement to Infringe upon the Sovereignty of the Republic of Lithuania by Using Violence A person who publicly incites infringement upon the sovereignty of the Republic of Lithuania by using violence –altering of its constitutional order, overthrowing of the legitimate government, making an attempt against its independence or infringement upon territorial integrity, formation of armed groups for these purposes or commission of other crimes provided for in this Chapter and having the aim of threatening the State of Lithuania shall be punished by a custodial sentence for a term of up to five years.

124 straipsnis. Neteisėtas disponavimas informacija, kuri yra valstybės paslaptis	Article 124. Unlawful Possession of the Information Constituting a State Secret
Tas, kas neteisėtai įgijo ar perleido informaciją, kuri yra Lietuvos Respublikos valstybės paslaptis, arba neteisėtai laikė materialius objektus, kurių turinys ar informacija apie juos yra Lietuvos Respublikos valstybės paslaptis, jeigu nebuvo šnipinėjimo požymių,	A person who unlawfully acquires or conveys the information constituting a state secret of the Republic of Lithuania or unlawfully holds in possession the material items whose content or information thereon constitutes a state secret of the Republic of Lithuania, in the absence of signs of espionage,
baudžiamas bauda arba areštu, arba laisvės atėmimu iki trejų metų.	shall be punished by a fine or by arrest or by a custodial sentence for a term of up to three years.
126 straipsnis. Valstybės paslapties praradimas	Article 126. Loss of a State Secret
1. Tas, kas sunaikino, sugadino ar prarado dėl tarnybos, darbo ar viešųjų funkcijų atlikimo jam patikėtą dokumentą, daiktą ar kitą materialų objektą, kurio turinys ar informacija apie jį yra Lietuvos Respublikos valstybės paslaptis,	1. A person who destroys, damages or loses a document, article or another material item entrusted to him through his service, work or in the course of performance of public functions whose content or information thereon constitutes a state secret of the Republic of Lithuania
baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba laisvės atėmimu iki dvejų metų.	shall be punished by community service or by a fine or by restriction of liberty or by a custodial sentence for a term of up to two years.
2. Šio straipsnio 1 dalyje numatyta veika yra nusikaltimas ir tais atvejais, kai ji padaryta dėl neatsargumo.	2. The act provided for in paragraph 1 of this Article shall be a crime also where it is committed through negligence.
154 straipsnis. Šmeižimas	Article 154. Libel
1. Tas, kas paskleidė apie kitą žmogų tikrovės neatitinkančią informaciją, galinčią paniekinti ar pažeminti tą asmenį arba pakirsti pasitikėjimą juo,	1. A person who spreads false information about another person that could arouse contempt for this person or humiliate him or undermine trust in him
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki vienerių metų.	shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to one year.
2. Tas, kas šmeižė asmenį, neva šis padarė sunkų ar labai sunkų nusikaltimą, arba per visuomenės informavimo priemonę ar spaudinyje,	2. A person who libels a person accusing him of commission of a serious or grave crime or in the media or in a publication

baudžiamas bauda arba areštu, arba laisvės atėmimu iki dvejų metų.	shall be punished by a fine or by arrest or by a custodial sentence for a term of up to two years.
3. Už šiame straipsnyje numatytas veikas asmuo atsako tik tuo atveju, kai yra nukentėjusio asmens skundas ar jo teisėto atstovo pareiškimas, ar prokuroro reikalavimas.	3. A person shall be held liable for the acts provided for in this Article only under a complaint filed by the victim or a statement by the legal representative thereof or at the prosecutor's request.
162 straipsnis. Vaiko išnaudojimas pornografijai	Article 162. Exploitation of a Child for Pornography
1. Tas, kas verbavo, vertė arba įtraukė vaiką dalyvauti pornografinio pobūdžio renginiuose, arba išnaudojo vaiką tokiems tikslams, arba išnaudojo vaiką pornografinei produkcijai gaminti, arba pelnėsi iš tokios vaiko veiklos,	1. A person who recruits, forces to participate or involves a child in pornographic events or exploits the child for such purposes or exploits the child for the production of pornographic material or gains profit from such activities of the child
baudžiamas laisvės atėmimu iki aštuonerių metų.	shall be punished by a custodial sentence for a term of up to eight years.
2. Tas, kas dalyvavo pornografinio pobūdžio renginyje, į kurį buvo įtrauktas vaikas,	2. A person who takes part in a pornographic event wherein a child is involved
baudžiamas bauda arba areštu, arba laisvės atėmimu iki dvejų metų.	shall be punished by a fine or by arrest or by a custodial sentence for a term of up to two years.
3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.	3. A legal entity shall also be held liable for the acts provided for in this Article.
168 straipsnis. Neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas	Article 168. Unauthorised Disclosure or Use of Information about a Person's Private Life
1. Tas, kas be asmens sutikimo viešai paskelbė, pasinaudojo ar kitų asmenų labui panaudojo informaciją apie kito žmogaus privatų gyvenimą, jeigu tą informaciją jis sužinojo dėl savo tarnybos ar profesijos arba atlikdamas laikiną užduotį, arba ją surinko darydamas šio kodekso 165–167 straipsniuose numatytą veiką,	1. A person who, without another person's consent, makes public, uses for his own benefit or for the benefit of another person information about the private life of another person, where he gains access to that information through his service or profession or in thecourse of performance of a temporary assignment or he collects it through the commission of an act provided for in Articles 165-167 of this Code,
baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.	shall be punished by community service or by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to three years.

2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo. 3. Už šiame straipsnyje numatytą veiką asmuo atsako tik tuo atveju, kai yra nukentėjusio asmens skundas ar jo teisėto atstovo pareiškimas, ar prokuroro reikalavimas.	2. A legal entity shall also be held liable for an act provided for in this Article. 3. A person shall be held liable for an act provided for in this Article only under a complaint filed by the victim ora statement by the legal representative thereof or at the prosecutor's request.
169 straipsnis. Diskriminavimas dėl tautybės, rasės, lyties, kilmės, religijos ar kitos grupinės priklausomybės Tas, kas atliko veiksmus, kuriais siekta žmonių grupei ar jai priklausančiam asmeniui dėl amžiaus, lyties, seksualinės orientacijos, neįgalumo, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų sutrukdyti lygiomis teisėmis su kitais dalyvauti politinėje, ekonominėje, socialinėje, kultūrinėje, darbo ar kitoje veikloje arba suvaržyti tokios žmonių grupės ar jai priklausančio asmens teises ir laisves, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.	Article 169. Discrimination on Grounds of Nationality, Race, Sex, Descent, Religion or Belonging to Other Groups A person who carries out the actions aimed at hindering, on grounds of age, sex, sexual orientation, disability, race, nationality, language, descent, social status, religion, convictions or views, a group of persons or a person belonging thereto to participate on a par with other persons in political, economic, social, cultural, labour or other activities or at restricting the rights and freedoms of such a group of persons or of the person belonging thereto shall be punished by community service or by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to three years.
170 straipsnis. Kurstymas prieš bet kokios tautos, rasės, etninę, religinę ar kitokią žmonių grupę 1. Tas, kas turėdamas tikslą platinti gamino, įsigijo, siuntė, gabeno, laikė dalykus, kuriuose tyčiojamasi, niekinama, skatinama neapykanta ar kurstoma diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl amžiaus, lyties, seksualinės orientacijos, neįgalumo, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų arba kurstoma smurtauti, fiziškai susidoroti su tokia žmonių grupe ar jai priklausančiu asmeniu, arba juos platino, baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki vienerių metų.	Article 170. Incitement against Any National, Racial, Ethnic, Religious or Other Group of Persons 1. A person who, for the purposes of distribution, produces, acquires, sends, transports or stores the items ridiculing, expressing contempt for, urging hatred of or inciting discrimination against a group of persons or a person belonging thereto on grounds of age, sex, sexual orientation, disability, race, nationality, language, descent, social status, religion, convictions or views or inciting violence, a physical violent treatment of such a group of persons or the person belonging thereto or distributes them shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to one year.

2. Tas, kas viešai tyčiojosi, niekino, skatino neapykantą ar kurstė diskriminuoti žmonių grupę ar jai priklausantį asmenį dėl amžiaus, lyties, seksualinės orientacijos, neįgalumo, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų,	2. A person who publicly ridicules, expresses contempt for, urges hatred of or incites discrimination against a group ofpersons or a person belonging thereto on grounds of age, sex, sexual orientation, disability, race, nationality, language, descent, social status, religion, convictions or views
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.	shall be punished by a fine or by restriction of liberty or by arrest or by acustodial sentence for a term of up to two years.
3. Tas, kas viešai kurstė smurtauti, fiziškai susidoroti su žmonių grupe ar jai priklausančiu asmeniu dėl amžiaus, lyties, seksualinės orientacijos, neįgalumo, rasės, tautybės, kalbos, kilmės, socialinės padėties, tikėjimo, įsitikinimų ar pažiūrų arba finansavo ar kitaip materialiai rėmė tokią veiklą,	3. A person who publicly incites violence or a physical violent treatment of a group of persons or a person belonging thereto on grounds of age, sex, sexual orientation, disability, race, nationality, language, descent, social status, religion, convictions or views or finances or otherwise supports such activities
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.	shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to three years.
4. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.	4. A legal entity shall also be held liable for the acts provided for in this Article.
170-2 straipsnis. Viešas pritarimas tarptautiniams nusikaltimams, SSRS ar nacistinės Vokietijos nusikaltimams Lietuvos Respublikai ar jos gyventojams, jų neigimas ar šiurkštus menkinimas	Article 170-2. Public Condonation of International Crimes, Crimes Committed by the USSR or Nazi Germany against the Republic of Lithuania or Inhabitants Thereof, Denial or Gross Trivialisation of the Crimes
1. Tas, kas viešai pritarė Lietuvos Respublikos ar Europos Sąjungos teisės aktais arba įsiteisėjusiais Lietuvos Respublikos ar tarptautinių teismų sprendimais pripažintiems genocido ar kitiems nusikaltimams žmoniškumui arba karo nusikaltimams, juos neigė ar šiurkščiai menkino, jeigu tai padaryta grasinančiu, užgauliu ar įžeidžiančiu būdu arba dėl to buvo sutrikdyta viešoji tvarka, taip pat tas, kas viešai pritarė SSRS ar nacistinės Vokietijos įvykdytai agresijai prieš Lietuvos Respubliką, SSRS ar nacistinės Vokietijos įvykdytiems Lietuvos Respublikos teritorijoje ar prieš Lietuvos Respublikos gyventojus genocido ar kitiems nusikaltimams žmoniškumui arba karo	1. A person who publicly condones the crimes of genocide or other crimes against humanity or war crimes recognised under legal acts of the Republic of Lithuania or the European Union or effective judgements passed by courts of the Republic of Lithuania or international courts, denies or grossly trivialises them, where this is accomplished in a manner which is threatening, abusive or insulting or which disturbs the public order, also a person who publicly condones the aggression perpetrated by the USSR or Nazi Germany against the Republic of Lithuania, the crimes of genocide or other crimes against humanity or war crimes committed by the USSR or Nazi Germany in the territory of

nusikaltimams, arba 1990–1991 metais įvykdytiems kitiems agresiją prieš Lietuvos Respubliką vykdžiusių ar joje dalyvavusių asmenų labai sunkiems ar sunkiems nusikaltimams Lietuvos Respublikai arba labai sunkiems nusikaltimams Lietuvos Respublikos gyventojams, juos neigė ar šiurkščiai menkino, jeigu tai padaryta grasinančiu, užgauliu ar įžeidžiančiu būdu arba dėl to buvo sutrikdyta viešoji tvarka,	the Republic of Lithuania or against the inhabitants of the Republic of Lithuania or other grave or serious crimes committed during 1990-1991 against the Republic of Lithuania by the persons perpetrating or participating in perpetration of the aggression against the Republic of Lithuania or grave crimes against the inhabitants of the Republic of Lithuania, denies or grossly trivialises them, where this is accomplished in a manner which is threatening, abusive or insulting or which disturbs the public order,
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų. 2. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.	shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to two years. 2. A legal entity shall also be held liable for the acts provided for in this Article.
171 straipsnis. Trukdymas atlikti religines apeigas ar religines iškilmes Tas, kas necenzūriniais žodžiais, įžūliais veiksmais, grasinimais, patyčiomis ar kitais nepadoriais veiksmais sutrikdė valstybės pripažintos religinės bendruomenės ar bendrijos pamaldas ar kitas apeigas arba iškilmes, padarė baudžiamąjį nusižengimą ir	Article 171. Disturbance of Religious Ceremonies or Religious Celebrations A person who, through the use of taboo words, carrying out of defiant actions, making threats, taunting or other indecent actions, disrupted the services or other ceremonies or celebrations held by a religious community or society recognised by the State shall be considered to have committed a misdemeanour and
baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu.	shall be punished by community service or by a fine or by restriction of liberty or by arrest.
191 straipsnis. Autorystės pasisavinimas 1. Tas, kas savo vardu išleido arba viešai paskelbė svetimą literatūros, mokslo ar meno kūrinį (įskaitant kompiuterių programas ir duomenų bazes) arba jo dalį,	Article 191. Misappropriation of Authorship 1. A person who publishes or publicly announces as his own a literary, scientific or artistic work (including computer software and databases) or a part thereof created by another person
baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų. 2. Tas, kas pasinaudodamas tarnybos padėtimi arba panaudodamas psichinę prievartą privertė literatūros, mokslo ar	shall be punished by community service or by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to two year. 2. A person who, by taking advantage of his official position or by resorting to mental coercion, forces the author of a literary,

meno kūrinio (įskaitant kompiuterių programas ir duomenų bazes) arba jo dalies autorių pripažinti kitą asmenį bendraautoriumi ar autoriaus teisių perėmėju arba atsisakyti autorystės teisės,	scientific or artistic work (including computer software and databases) or a part thereof to acknowledge another person as the co-author or successor to author's rights or to renounce the right of authorship
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.	shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to three years.
3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.	3. A legal entity shall also be held liable for the acts provided for in this Article.
192 straipsnis. Literatūros, mokslo, meno kūrinio ar gretutinių teisių objekto neteisėtas atgaminimas, neteisėtų kopijų platinimas, gabenimas ar laikymas	Article 192. Unlawful Reproduction of a Literary, Scientific or Artistic Work or an Object of Related Rights, Distribution, Transportation or Storage of Illegal Copies Thereof
1. Tas, kas neteisėtai atgamino literatūros, mokslo ar meno kūrinį (įskaitant kompiuterių programas ir duomenų bazes) ar gretutinių teisių objektą arba jų dalį komercijos tikslais arba platino, gabeno ar laikė komercijos tikslais neteisėtas jų kopijas, jeigu kopijų bendra vertė pagal teisėtų kopijų, o kai jų nėra, pagal atgamintų kūrinių originalų kainas viršijo 100 MGL dydžio sumą,	1. A person who unlawfully reproduces a literary, scientific or artistic work (including computer software and databases) or an object of related rights or a part thereof for commercial purposes or distributes, transports or stores for commercial purposes illegal copies thereof, where the total value of the copies exceeds, according to the prices of legal copies or, in the absence thereof, according to the prices of originals of the reproduced works, the amount of 100 MSLs,
baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.	shall be punished by community service or by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to two year.
2. Tas, kas padarė šio straipsnio 1 dalyje numatytą veiką, jeigu neteisėtų kopijų bendra vertė pagal teisėtų kopijų, o kai jų nėra, pagal atgamintų kūrinių originalų kainas viršijo 250 MGL dydžio sumą,	2. A person who commits the act indicated in paragraph 1 of this Article, where the total value of the illegal copies exceeds, according to the prices of legal copies or, in the absence thereof, according to the prices of originals of the reproduced works, the amount of 250 MSLs,
baudžiamas bauda arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki trejų metų.	shall be punished by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to three years.
3. Už šiame straipsnyje numatytas veikas atsako ir juridinis asmuo.	3. A legal entity shall also be held liable for the acts provided for in this Article.

193 straipsnis. Informacijos apie autorių teisių ar gretutinių teisių valdymą sunaikinimas arba pakeitimas	Article 193. Destruction or Alteration of Information about Management of Author's Rights or Related Rights
1. Tas, kas be autorių teisių ar gretutinių teisių subjekto leidimo komercijos tikslais sunaikino arba pakeitė informaciją apie autorių teisių ar gretutinių teisių valdymą, jeigu pagal tą informaciją identifikuojamas kūrinys, kūrinio autorius, kitas autorių teisių subjektas arba atlikėjas, kūrinio atlikimas, fonograma, fonogramos gamintojas, kitas gretutinių teisių subjektas, taip pat informaciją apie kūrinio, jo atlikimo ar fonogramos naudojimo sąlygas ir tvarką, įskaitant visus skaičius ar kodus, perteikiančius kūrinio, atlikimo įrašo ar fonogramos egzemplioriuose pažymėtą arba jų viešo paskelbimo metu pateikiamą informaciją,	1. A person who, without authorisation of the entity of author's rights or related rights and for commercial purposes, destroys or alters information about management of author's rights or related rights, where this information helps to identify a work, the author of the work, another entity of author's rights or the performer, performance of the work, a phonogram, the producer of the phonogram, another entity of related rights, also information about the terms and conditions of and procedure for using the work, performance thereof or the phonogram, including all figures or codes communicating the information indicated in copies of the work, performance record or the phonogram or presented at the time of their publication
baudžiamas bauda arba areštu, arba laisvės atėmimu iki vienerių metų.	shall be punished by a fine or by arrest or by a custodial sentence for a term of up to one year.
2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.	2. A legal entity shall also be held liable for an act provided for in this Article.
194 straipsnis. Neteisėtas autorių teisių ar gretutinių teisių techninių apsaugos priemonių pašalinimas	Article 194. Unlawful Removal of Technical Protection Means of Author's Rights or Related Rights
1. Tas, kas neteisėtai pašalino bet kokias technines apsaugos priemones, kurias autorių teisių ar gretutinių teisių subjektai naudoja savo teisėms įgyvendinti ar apsaugoti, arba komercijos tikslais gamino, importavo, eksportavo, laikė, gabeno ar platino galimybę pašalinti tas technines apsaugos priemones suteikiančius prietaisus (dekoderius, dekodavimo korteles ar kitokius prietaisus) arba programinę įrangą, slaptažodžius, kodus ar kitokius panašius duomenis,	1. A person who unlawfully removes any technical protection means used by entities of author's rights or related rights for the exercise or protection of their rights or produces, imports, exports, stores, transports or distributes for commercial purposes the devices providing a possibility to remove the technical protection means (decoders, decoding cards or other devices) or a software, passwords, codes or other similar data
baudžiamas bauda arba areštu, arba laisvės atėmimu iki dvejų metų.	shall be punished by a fine or by arrest or by a custodial sentence for a term of up to two years.

2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.	2. A legal entity shall also be held liable for an act provided for in this Article.
195 straipsnis. Pramoninės nuosavybės teisių pažeidimas 1. Tas, kas pažeidė išimtines patento savininko ar dizaino savininko teises arba juridinio asmens teisę į juridinio asmens pavadinimą, baudžiamas bauda arba areštu, arba laisvės atėmimu iki dvejų metų. 2. Už šiame straipsnyje numatytą veiką atsako ir juridinis asmuo.	Article 195. Violation of Industrial Property Rights 1. A person who violates the exclusive rights of a patent owner or a design owner or the right of a legal entity to the legal entity's name shall be punished by a fine or by arrest or by a custodial sentence for a term of up to two years. 2. A legal entity shall also be held liable for an act provided for in this Article.
211 straipsnis. Komercinės paslapties atskleidimas Tas, kas atskleidė komercine paslaptimi laikomą informaciją, kuri jam buvo patikėta ar kurią jis sužinojo dėl savo tarnybos ar darbo, jeigu ši veika padarė didelės turtinės žalos nukentėjusiam asmeniui, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu, arba laisvės atėmimu iki dvejų metų.	Article 211. Disclosure of a Commercial Secret A person who discloses the information considered to be a commercial secret which was entrusted to him or which he accessed through his service or work, where this act incurs major property damage to the victim, shall be punished by community service or by a fine or by restriction of liberty or by arrest or by a custodial sentence for a term of up to two years.
309 straipsnis. Disponavimas pornografinio turinio dalykais 1. Tas, kas turėdamas tikslą platinti pagamino ar įsigijo arba platino pornografinio turinio dalykus, baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba laisvės atėmimu iki vienerių metų. 2. Tas, kas pagamino, įgijo, laikė, demonstravo, reklamavo, siūlė arba platino pornografinio turinio dalykus, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas, arba pasinaudodamas informacinėmis ir ryšių technologijomis ar kitomis priemonėmis įgijo ar suteikė prieigą	Article 309. Possession of Pornographic Material 1. A person who, for the purpose of distribution, produces or acquires pornographic material or distributes such material shall be punished by community service or by a fine or by restriction of liberty or by a custodial sentence for a term of up to one year. 2. A person who produces, acquires, stores, demonstrates, advertises, offers or distributes pornographic material displaying a child or presenting a person as a child or, by means of information and communications technologies and other means, acquires or provides access to

prie pornografinio turinio dalykų, kuriuose vaizduojamas vaikas arba asmuo pateikiamas kaip vaikas, baudžiamas bauda arba laisvės atėmimu iki ketverių metų.	pornographic material displaying a child or presenting a person as a child, shall be punished by a fine or by a custodial sentence for a term of up to four years.
3. Tas, kas turėdamas tikslą platinti pagamino ar įsigijo arba platino didelį kiekį pornografinio turinio dalykų, kuriuose vaizduojamas mažametis vaikas, baudžiamas laisvės atėmimu iki penkerių metų.	3. A person who, for the purpose of distribution, produces or acquires or distributes a large quantity of pornographic material displaying a young child shall be punished by a custodial sentence for a term of up to five years.
4. Tas, kas demonstravo ar reklamavo pornografinio turinio dalykus, padarė baudžiamąjį nusižengimą ir baudžiamas viešaisiais darbais arba bauda, arba laisvės apribojimu, arba areštu.	4. A person who demonstrates or advertises pornographic material shall be considered to have committed a misdemeanour and shall be punished by community service or by a fine or by restriction of liberty or by arrest.
5. Už šio straipsnio 1, 2 ir 3 dalyse numatytas veikas atsako ir juridinis asmuo.	5. A legal entity shall also be held liable for the acts provided for in paragraphs 1, 2 and 3 of this Article.
LIETUVOS RESPUBLIKOS CIVILINIS KODEKSAS	THE CIVIL CODE OF THE REPUBLIC OF LITHUANIA
2.22 straipsnis. Teisė į atvaizdą 1. Fizinio asmens nuotrauka (jos dalis), portretas ar kitoks atvaizdas gali būti atgaminami, parduodami, demonstruojami, spausdinami, taip pat pats asmuo gali būti fotografuojamas tik jo sutikimu. Po asmens mirties tokį sutikimą gali duoti jo sutuoktinis, tėvai ar vaikai. 2. Asmens sutikimo nereikia, jeigu šie veiksmai yra susiję su visuomenine asmens veikla, jo tarnybine padėtimi, teisėsaugos institucijų reikalavimu arba jeigu fotografuojama viešoje vietoje. Tačiau asmens nuotraukos (jos dalies), padarytos šiais atvejais, negalima demonstruoti, atgaminti ar parduoti, jeigu tai pažemintų asmens garbę, orumą ar dalykinę reputaciją.	Article 2.22. Right to an Image 1. Photograph (or its part) or some other image of a natural person may be reproduced, sold, demonstrated, published and the person may be photographed only with his consent. Such consent after natural person's death may be given by his spouse, parents or children. 2. Where such acts are related to person's public activities, his official post, request of law enforcement agencies or where a person is photographed in public places, consent of a person shall not be required. Person's photograph (or its part) produced under the said circumstances, however, may not be demonstrated, reproduced or sold if those acts were to abase person's honour, dignity or damage his professional reputation.

3. Fizinis asmuo, kurio teisė į atvaizdą buvo pažeista, turi teisę teismo tvarka reikalauti nutraukti tokius veiksmus bei atlyginti turtinę ir neturtinę žalą. Po asmens mirties tokį ieškinį turi teisę pareikšti jo sutuoktinis, vaikai ir tėvai.	3. Natural person whose right to image has been infringed enjoys the right to request the court to oblige the discontinuance of the said acts and redressing of the property and non-pecuniary damage. After person's death, such claim may be presented by his spouse, children and parents.
2.23 straipsnis. Teisė į privatų gyvenimą ir jo slaptumą 1. Fizinio asmens privatus gyvenimas neliečiamas. Informacija apie asmens privatų gyvenimą gali būti skelbiama tik jo sutikimu. Po asmens mirties tokį sutikimą gali duoti jo sutuoktinis, tėvai ar vaikai. 2. Privataus gyvenimo pažeidimu laikomas neteisėtas įėjimas į asmens gyvenamąsias ir kitokias patalpas, aptvertą privačią teritoriją, neteisėtas asmens stebėjimas, neteisėtas asmens ar jo turto apieškojimas, asmens telefoninių pokalbių, susirašinėjimo ar kitokios korespondencijos bei asmeninių užrašų ir informacijos konfidencialumo pažeidimas, duomenų apie asmens sveikatos būklę paskelbimas pažeidžiant įstatymų nustatytą tvarką bei kitokie neteisėti veiksmai. 3. Draudžiama rinkti informaciją apie privatų asmens gyvenimą pažeidžiant įstatymus. Asmuo turi teisę susipažinti su apie jį surinkta informacija, išskyrus įstatymų nustatytas išimtis. Draudžiama skleisti surinktą informaciją apie asmens privatų gyvenimą, nebent, atsižvelgiant į asmens einamas pareigas ar padėtį visuomenėje, tokios informacijos skleidimas atitinka teisėtą ir pagrįstą visuomenės interesą tokią informaciją žinoti. 4. Privataus asmens gyvenimo duomenų, nors ir atitinkančių tikrovę, paskelbimas, taip pat asmeninio susirašinėjimo paskelbimas pažeidžiant šio straipsnio 1 ir 3 dalyse nustatytą tvarką, taip pat įėjimas į asmens gyvenamąjį būstą be jo sutikimo, išskyrus įstatymų numatytas išimtis, asmens privataus	Article 2.23. Right to Privacy and Secrecy 1. Privacy of natural person shall be inviolable. Information on person's private life may be made public only with his consent. After person's death the said consent may be given by person's spouse, children and parents. 2. Unlawful invasion of person's dwelling or other private premises as well as fenced private territory, keeping his private life under observation, unlawful search of the person or his property, intentional interception of person's telephone, post or other private communications as well as violation of the confidentiality of his personal notes and information, publication of the data on the state of his health in violation of the procedure prescribed by laws and other unlawful acts shall be deemed to violate person's private life. 3. Establishment of a file on another person's private life in violation of law shall be prohibited. A person may not be denied access to the information contained in the file except as otherwise provided by the law. Dissemination of the collected information on the person's private life shall be prohibited unless, taking into consideration person's official post and his status in the society, dissemination of the said information is in line with the lawful and well-grounded public interest to be aware of the said information. 4. Public announcement of facts of private life, however truthful they may be, as well as making private correspondence public in violation of the procedure prescribed in paragraphs 1 and 3 of the given Article as well as invasion of person's dwelling without his consent except as otherwise provided by

gyvenimo stebėjimas ar informacijos rinkimas apie jį pažeidžiant įstatymą bei kiti neteisėti veiksmai, kuriais pažeidžiama teisė į privatų gyvenimą, yra pagrindas pareikšti ieškinį dėl tokiais veiksmais padarytos turtinės ir neturtinės žalos atlyginimo.	the law, keeping his private life under observation or gathering of information about him in violation of law as well as other unlawful acts, infringing the right to privacy shall form the basis for bringing an action for repairing the property and non-pecuniary damage incurred by the said acts.
5. Šio straipsnio 1 ir 3 dalyse numatyti apribojimai, susiję su informacijos apie asmenį skelbimu ir rinkimu, netaikomi, kai tai daroma motyvuotu teismo sprendimu.	5. Where the said acts are committed on the basis of reasoned judgement of the court, restrictions imposed on the publication and collecting of information about the person which are laid down in the provisions of paragraphs 1 and 3 of the given Article shall not be applied.
2.24 straipsnis. Asmens garbės ir orumo gynimas	Article 2.24. Protection of Honour and Dignity
1. Asmuo turi teisę reikalauti teismo tvarka paneigti paskleistus duomenis, žeminančius jo garbę ir orumą ir neatitinkančius tikrovės, taip pat atlyginti tokių duomenų paskleidimu jam padarytą turtinę ir neturtinę žalą. Po asmens mirties tokią teisę turi jo sutuoktinis, tėvai ir vaikai, jeigu tikrovės neatitinkančių duomenų apie mirusįjį paskleidimas kartu žemina ir jų garbę bei orumą. Preziumuojama, jog paskleisti duomenys neatitinka tikrovės, kol juos paskleidęs asmuo neįrodo priešingai.	1. A person shall have the right to demand refutation in judicial proceedings of the publicised data, which abase his honour and dignity and which are erroneous as well as redress of the property and non-pecuniary damage incurred by the public announcement of the said data. After person's death this right shall pass on to his spouse, parents and children if the public announcement of erroneous data about the deceased person abases their honour and dignity as well. The data, which was made public, shall be presumed to be erroneous as long as the person who publicised them proves the opposite.
2. Jeigu tikrovės neatitinkantys duomenys buvo paskleisti per visuomenės informavimo priemonę (spaudoje, televizijoje, radijuje ir pan.), asmuo, apie kurį šie duomenys buvo paskleisti, turi teisę surašyti paneigimą ir pareikalauti, kad ta visuomenės informavimo priemonė šį paneigimą nemokamai išspausdintų ar kitaip paskelbtų. Visuomenės informavimo priemonė šį paneigimą privalo išspausdinti ar kitaip paskelbti per dvi savaites nuo jo gavimo dienos. Visuomenės informavimo priemonė turi teisę atsisakyti spausdinti ar paskelbti paneigimą tik tuo atveju, jeigu paneigimo turinys prieštarauja gerai moralei.	2. Where erroneous data were publicised by a mass medium (press, television, radio etc.) the person about whom the data was publicised shall have the right to file a refutation and demand the given mass medium to publish the said refutation free of charge or make it public in some other way. The mass medium shall have to publish the refutation or make it public in some other way in the course of two weeks from its receipt. Mass medium shall have the right to refuse to publish the refutation or make it public only in such cases where the content of the refutation contradicts good morals.

3. Reikalavimą atlyginti turtinę ir neturtinę žalą nagrinėja teismas, nepaisydamas to, ar tokius duomenis paskleidęs asmuo juos paneigė, ar ne.	3. The request to redress the property or non-property non-pecuniary damage shall be investigated by the court irrespective of the fact whether the person who has disseminated such data refuted them or not.
4. Jeigu visuomenės informavimo priemonė atsisako spausdinti ar kitaip paskelbti paneigimą arba to nepadaro per šio straipsnio 2 dalyje nustatytą terminą, asmuo įgyja teisę kreiptis į teismą šio straipsnio 1 dalyje nustatyta tvarka. Duomenų, neatitinkančių tikrovės ir žeminančių kito asmens reputaciją, paneigimo tvarką ir terminus tokiu atveju nustato teismas.	4. Where a mass medium refuses to publish the refutation or make it public in some other way or fails to do it in the term provided in paragraph 2 of the given Article, the person gains the right to apply to court in accordance with the procedure established in paragraph 1 of the given Article. The court shall establish the procedure and the term for the refutation of the data, which were erroneous or abased other person's reputation.
5. Visuomenės informavimo priemonė, paskleidusi asmens reputaciją žeminančius ir tikrovės neatitinkančius duomenis, privalo atlyginti asmeniui padarytą turtinę ir neturtinę žalą tik tais atvejais, kai ji žinojo ar turėjo žinoti, jog paskleisti duomenys neatitinka tikrovės, taip pat kai tuos duomenis paskelbė jos darbuotojai ar duomenys paskleisti anonimiškai, o visuomenės informavimo priemonė atsisako nurodyti tuos duomenis pateikusį asmenį. Visais kitais atvejais turtinę ir neturtinę žalą privalo atlyginti duomenis paskleidęs asmuo ir jo veikla.	5. The mass medium, which publicised erroneous data abasing person's reputation shall have to redress property and non-pecuniary damage incurred on the person only in those cases, when it knew or had to know that the data were erroneous as well as in those cases when the data were made public by its employees or the data was made public anonymously and the mass medium refuses to name the person who supplied the said data.
6. Paskleidęs tikrovės neatitinkančius duomenis asmuo atleidžiamas nuo civilinės atsakomybės, jeigu tie duomenys yra paskelbti apie viešą asmenį bei jo valstybinę ar visuomeninę veiklą, o juos paskelbęs asmuo įrodo, kad jis veikė sąžiningai siekdamas supažindinti visuomenę su tuo asmeniu ir jo veikla.	6. The person who made a public announcement of erroneous data shall be exempted from civil liability in cases when the publicised data is related to a public person and his state or public activities and the person who made them public proves that his actions were in good faith and meant to introduce the person and his activities to the public.
7. Jeigu nevykdomas teismo sprendimas, įpareigojantis paneigti tikrovės neatitinkančius duomenis, žeminančius asmens garbę ir orumą, teismas nutartimi gali išieškoti iš atsakovo baudą už kiekvieną teismo sprendimo nevykdymo dieną. Baudos dydį nustato teismas. Ji yra išieškoma ieškovo naudai, nepaisant neturtinės žalos atlyginimo.	7. Where the court judgement, which obliges the refutation of erroneous data abasing person's honour and dignity, is not executed , the court may issue an order to recover a fine from the defendant for each day of default. The amount of the fine shall be established by the court. It shall be recovered for the benefit of the defendant

	irrespective of the redress for the inflicted damage.
8. Šio straipsnio taisyklės taip pat yra taikomos ginant pažeistą juridinio asmens dalykinę reputaciją.	8. Provisions of the given article shall, too, be applied to protect the tarnished professional reputation of a legal person.
9. Šio straipsnio taisyklės netaikomos teismo proceso dalyviams, kurie už teismo posėdžio metu pasakytas kalbas bei teismo dokumentuose paskelbtus duomenis neatsako.	9. Provisions of the given article shall not be applied to those participants of judicial proceedings who are not held responsible for the speeches delivered at court hearings or data made public in judicial documents.

Bibliography

English titles

Legislation

The Constitution of the Republic of Lithuania, Article 25. Source: https://www.lrs.lt/home/Konstitucija/Constitution.htm.

The Criminal Code of the Republic of Lithuania, Article 170. Source: https://e-seimas.lrs.lt/portal/legalActPrint/lt?jfwid=q8i88l10w&documentId=a84fa232877611e5bca4ce385a9b7048&category=TAD.

The Constitution of the Republic of Lithuania, Article 25. Source: https://www.lrs.lt/home/Konstitucija/Constitution.htm.

The Civil Code of the Republic of Lithuania, Article 1.137. Source: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.245495.

Law on the Provision of Information to the Public, Article 4. Source: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2865241206f511e687e0fbad81d55a7c?jfwid=1clcwosx33.

Law on the Provision of Information to the Public, Article 7, 10. Source: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/2865241206f511e687e0fbad81d55a7c?jfwid=1clcwosx33.

Directive 2000/31/EC articles 12-14. Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=LT

Digital resources

https://hubshout.com/?Mirror-Site&AID=1468.

Case law

The Constitutional Court ruling of 13 February 1997. Source: https://hudoc.echr.coe.int/eng#{"itemid":["001-180506"]}.

The Constitutional Court ruling of 10 March 1998. Source: https://hudoc.echr.coe.int/eng#{"itemid":["001-180506"]}.

European Court of Human Rights case of Sekmadienis Ltd. v. Lithuania of 30 January 2018. Source: https://hudoc.echr.coe.int/eng#{"itemid":["001-180506"]}.

Supreme Court of Lithuania case No.: e3K-3-236-969/2019

Beizaras and Levickas v. Lithuania (no. 41288/15, 14 January 2020) (https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200344%22]})

Lithuanian titles

Legislation

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. Source: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29193?jfwid=24tshwf64

Lietuvos Respublikos Kultūros ministro 2019 m. lapkričio 25 d. Nr. ĮV-771 įsakymas *Dėl Privalomų nurodymų taikymo interneto prieigos paslaugų teikėjams tvarkos aprašo patvirtinimo*. Source: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/eb6513f3108b11eaa1dda5669c1a32a1 ?jfwid=15vz32tkeb

Digital resources

https://vdai.lrv.lt/lt/naujienos/bendrasis-duomenu-apsaugos-reglamentas-ginama-teise-susipazinti-su-savo-asmens-duomenimis

https://www.vz.lt/rinkodara/2019/04/01/kaip-veiks-neleistino-turinio-blokavimasinternete

https://www.delfi.lt/m360/naujausi-straipsniai/lrtk-igaliota-blokuoti-veidrodines-interneto-svetaines-kuriose-skelbiamas-nelegalus-turinys.d?id=82961111

https://manoteises.lt/straipsnis/neapykantos-kurstymas-internete-zmogaus-teise-i-oruma-saviraiskos-laisves-uzribyje/

Case law

Lietuvos Aukščiausiasis teimas, byla Nr. e3K-3-236-969/2019

ELSA Malta

Contributors

National Coordinator

Nicole Borg

National Academic Coordinator

Julia Aquilina

National Researchers

Cristina Consoli Chetcuti Ganado

Daphne Vassallo

Diane Cutajar

Joseph Axisa

Raoul Ciappara

National Linguistic Editor

Josefa Muscat

National Technical Editor

Francesca Fenech

National Academic Supervisor

Dr. Nigel Micallef

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

One of the fundamental human rights is freedom of expression. In fact, it is one of the human rights found under the European Convention on Human Rights (ECHR) expressed by Article 10. Under this convention, everyone has the Right to Express their opinions together with giving your own ideas. It is expressly stated under this Article, that just because it gives the right for everyone to have freedom of expression, States can still control this Right; such as restricting television broadcasting according to the national legislation of the State. Already this implies that there is a form of restriction on this Right as the State, for example, has to grant a licence for broadcasting purposes.

Malta ratified the European Convention on Human Rights, in 1967, therefore it also includes freedom of expression. This right is also protected under Article 41 sub-article 1 of the Constitution of Malta, 'Except with his own consent or by way of parental discipline, no person shall be hindered in the enjoyment of his freedom of expression.' Under Article 32 of the Constitution one also finds that freedom of expression is applicable to anyone, 'whatever his race, place of origin, political opinions, colour, creed, sex, sexual orientation or gender identity, but subject to respect for the rights and freedoms of others and for the public interest.' The fact that both the ECHR and the Maltese constitution have enshrined in them emphasises that Malta has dual protection and its protection highlights the importance of it in a country, especially a democratic one like Malta.

The right of freedom of expression is also enshrined in the Data Protection Act, Chapter 586 of the Laws of Malta. This act was enacted after the EU Regulation on General Data Protection Regulation. Article 85 of such regulation expressly states how Member States are to enact the Right of Freedom of Expression together with the right of protection of personal data. It goes on to explain that even though some information can be processed by journalists or academic purposes, it does not mean that they have the full rights over them, as they still have to follow what the national legislation says and protect the information they receive. This is also found under Article 9(1) of the Data Protection Act which states that personal data, which is processed for freedom of expression and information together with the processing for journalists and academic reasons, is exempt from complying with the rules set out under the regulation. The proviso of such an Article explains that even though these are exempt from the Regulation's provisions, the controller has the duty to check that the information

processed is for a legitimate purpose and is always made in the interest of the public and not for any private interest.[1300]

In Malta, generally there are no limitations on different opinions and beliefs between the people, both citizens in Malta and those visiting the country. Of course, there are laws which prohibit any hatred which people may have towards people who have a different opinion or belief than them. One has to remember that the right for freedom of expression is not an absolute right as one has duties and responsibilities accompanied with this right. In fact the Maltese Press Act, establishes the offences in regard to the publications and distributing of material which insult, offend and show hatred towards others because of the person's gender, sexual orientation, religion, race, language, beliefs and much more.[1301] This act focuses on hate speech in Malta and the offences related to them which are also found in the Criminal Code. It does not only focus on speeches given to the other citizens and the public but also towards any public officials. Therefore, even though Freedom of Expression is a Right which everyone is entitled to in Malta, whether being a Maltese citizen or a foreigner, the Criminal Code still limits how this right is used. If it is used to instil hatred or offend someone, because of any physical appearance or beliefs or sexual orientations, the person doing so is liable for an offence.

Any defamatory words used which are liable to cause harm to the person, are considered to be a limit to the Right of Freedom of Expression. The Media and Defamation Act 2018 came into force and put an end to criminal libels; any words which are published or written online or on any kind of social media which can slander someone is not considered to be a criminal offence. People filing garnishee orders against journalists was also put to an end.[1302] This is a protection against the limitation of the Right of Freedom of Expression. The legislator here wanted to safeguard journalists, especially from expressing their opinions and ideas about different things and not getting criminalised for what they are saying. Another protection against the limitations of freedom of expression is found in Article 22 of the Media and Defamation Act 2018, which safeguards journalists, editors, authors and publishers. It gives them the right not to disclose the source from where they got the information they published, in a newspaper or something which is broadcasted. Once again, this is highlighting the importance of freedom of expression because it gives them the Right to

[1300] Article 9, Data Protection Act, Laws of Malta.

[1301] Article 6, Press Act, Laws of Malta.

[1302] 'Criminal Libel Is History As New Media Law Comes Into Force' (*Times of Malta*, 2020) <https://timesofmalta.com/articles/view/criminal-libel-is-history-as-new-media-law-comes-into-force.679111> accessed 18 February 2020.

express their own opinions and not get criminalised for it. Of course, if such information is needed to establish a series of facts in a court case, or because it is necessary in the interest of the public and the public's safety and national security, then such sources need to be disclosed.[1303]

The famous case of Police vs Massimo Gorla (1986), is an important one to mention when one is talking about the right of freedom of expression. At the time of this case, Malta had a Foreign Interference Act which was enacted in 1982. This act stated that foreigners could not participate in any political meetings in Malta and when Gorla was invited to give a speech, he was arraigned in the Criminal Court, but this court referred it to the Constitutional Court as it was in violation of a fundamental human right. The court stated that the right of freedom of expression is not only a right which Maltese people enjoy, but also all foreigners who are in Malta; thus 'any person in Malta' benefits from this fundamental human right. Nowadays, all foreigners are on the same level as Maltese people when it comes to exercising their Right of Freedom of Expression.

This fundamental human right is one of the most important rights there is, as it gives you the chance to express yourself and not be penalised for it. The fact that Malta has dual protection on this right due to the European Convention of Human Rights and the national legislation, establishes the importance this right has in Malta. This fundamental human right should not be taken for granted and one must remember that with it comes to duty, one must not exceed it and be responsible about the things one says.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

The Media and Defamation Act regulates internet censorship in the Maltese jurisdiction. This act was enacted on the 24 April 2018 and replaced the previous Press Act (which was Chapter 248 of the Laws of Malta). Conversely, the Press Act has been repealed and the new 'Media and Defamation Act' has been enacted. It is good to take note of the fact that the new act contains substantial excerpts from its predecessor i.e. the Press Act. The introduction of this new act gave rise to controversy, so much so that thousands of Maltese citizens held a protest against the new Media and Defamation prior to its enactment.

[1303] Article 23, Act No. XI of 2018, Laws of Malta.

This new piece of legislation addresses concepts which were not addressed by the previous Press Act. It makes reference to the internet, online news portals, and journalists who predominantly use the internet as a means to express their opinions, discoveries and investigations. These were not referred to or mentioned by the Press Act, thus the new law has added a tinge of technological progress to the Maltese corpus juris. For example, the law no longer refers to 'printed matter', but it uses the terminology of 'written media'.

The Media and Defamation Act abolished criminal libel and updated the laws regarding the offence of defamation. It also envisages that current criminal proceedings are to be terminated upon the enactment of the law. Even though it abolished criminal libel, it introduced a new way of how civil remedies can be applicable to the offence of slander, which is defined by the new law as, 'defamation by spoken words uttered with malice'. Thus, when a person posts words on the internet which slander a person, these do not constitute a criminal offence.

Where court proceedings are initiated in terms of the aforementioned act, the court has the authority to order the defendant to pay a sum of not more than 11,640 euros in the form of moral damages or actual damages. However, with regards to proceedings regarding slander, the court may only grant moral damages at a maximum of 5,000 euros.

An honourable mention with regards to online regulation is Chapter 399 of the Laws of Malta (The Electronic Communications (Regulation) Act, which regulates any form of communication made electronically.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

This form of regulation is not present under Maltese law. Presently, we do not have any form of specific legislation which envisages the blocking, filtering and removal of internet content. However, there are some laws which may be used in a court of law to justify the taking down of internet content.

Furthermore, the Data Protection Act (Chapter 440 of the Laws of Malta) also establishes a few circumstances where internet content which is infringing the law may be either blocked or removed totally (through its destruction). This is done through the Data Protection Commissioner, who is vested with the power to carry out the aforementioned acts.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In the Maltese jurisdiction there is no private company which renders the service of taking down or blocking internet content. However, Internet service providers collaborate with the Cyber Crime Unit on a daily basis to block or filter websites which show illegal content or have, as their purpose, the provision of illegal items (contraband).

Among the various types of illegal content is child pornography. The Cospol Internet Related Child Abusive Material Project was initiated by the European Police Chief Task Force. It has as its main aim the fighting of the exploitation and abuse of minors done through the distribution of images via different internet channels.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

The right to be forgotten, which is also known as the right of erasure, is found in Article 17 of the EU Regulation 2016/679 on the protection of natural persons, with regard to the processing of personal data and on the free movement of such data. It is one of the rights which the data subject has, when personal data about himself/herself is collected. This regulation is applicable to Member States; therefore, Malta follows the rules and regulations found under it.

This right was introduced in Malta after the Regulation came into effect. Before this, the right to be forgotten or deleted were not mentioned in Maltese laws whereas now the country follows the laws established by this Regulation, when it comes to speaking of this right and following its rule. Article 17 of the EU Regulation on General Protection Data, enables people to have data deleted about them when the data is no longer necessary needed for the purpose which it was needed it in the first place; when they withdraw their consent from having their data processed, apart from when having any form of legal criteria in which the data is needed nonetheless; if the data was unlawfully processed, the data subject has a right to ask the controller to erase the data about him; and when the data has to be deleted because it goes against any obligation given by the EU or by Member States' laws.[1304] Malta adhered to this regulation in May 2018,

[1304] Data Protection: EU Citizens' Right to be Forgotten Limited to EU Territory - Iuris Malta (Iuris Malta, 2020) <http://iurismalta.com/data-protection-eu-citizens-right-forgotten-limited-eu-territory/>

therefore the country follows the rules and obligations established under this regulation.

In 2019, the Minister of Justice of Malta expressly stated that the right to be forgotten has to be respected due to the fact that we are not living in an era where the rights of the citizens are not respected. We are in a generation where these rights have to be respected whether or not they are enshrined in law. These rights came about with the Right of Privacy, in fact the Minister of Justice explained that if we follow the Right of Privacy, this means that the right to be forgotten should be respected and included as well.[1305]

A situation which has occurred in Malta along the past few years, is about the court's database which was made online in the year 2000. A number of people have been asking the court to remove a judgement from the database which has their name on it in order to safeguard themselves from being exposed to the public eye. Even though, technically, Malta has no specific legislation on the right to be forgotten, the court is still accepting and processing these requests made by following Article 17 of the EU Regulation. However, there is still an ongoing controversy in this regard, as justice can be made if the public can see it to be made. Therefore, they need to refer to these court judgements and if they are erased, it hinders this aspect. Moreover, this can also be said as going against a clause found in Article 17 of the Regulation, which specifically says that the right to be forgotten does not apply to the Right of Freedom of Expression and information. Therefore, the fact that information is being erased from judgements is said to be going against this clause.

One needs to remember that the right to be forgotten is not an absolute right, but it is given in the interest of the public and whether or not the data held is needed for that purpose anymore.[1306] Therefore, this right should also be balanced with the right of the public interest because the public interest should always be taken into consideration when deciding whether or not the data of a subject should be deleted. Freedom of expression and information, as well as,

accessed 17 February 2020.

1305 Albert Galea, Court Judgments Removed From Internet: Right to Be Forgotten Must Be Respected – Bonnici - The Malta Independent (Independent.com.mt, 2020) <https://www.independent.com.mt/articles/2019-05-17/local-news/Court-judgments-removed-from-internet-Right-to-be-forgotten-must-be-respected-Bonnici-6736208252> accessed 15 February 2020.

1306 Matthew Vella, 'Erasing The Right To Know: Maltese Courts Applying Restrictive Interpretation of Privacy Rules' (MaltaToday.com.mt, 2020) <https://www.maltatoday.com.mt/news/national/86330/erasing_the_right_to_know_maltese_courts_applying_restrictive_interpretation_of_privacy_rules#.XkftVS3MxQI> accessed 17 February 2020.

the legal obligations and reasons why the data is held should also be regarded before exercising the right to be forgotten.

6. How does your country regulate the liability of internet intermediaries?

In Malta, the Electronic Commerce Act under Part VI regulates the 'secondary liability' of internet intermediaries. This Act lays down a set of special liability rules which can be traced back to the e-Commerce Directive which introduced this 'special liability regime' in the year 2000. These rules consist of the three instances in which intermediary service providers are exempt from liability subject to the satisfaction of certain conditions. These three instances are, where intermediaries provide mere conduit, caching and hosting services.

There are three main rules which govern special liability. The first regulates mere conduit service providers[1307]. This entails an information society service which is provided with the purpose of transmitting information within a communication network. Such information is provided by the recipient of the service. The service provider shall not be held liable other than a prohibitory injunction for the information transmitted. The acts of transmission and provision of access, in and to a communication network, include the automatic intermediate and transient storage of the information transmitted. This is, as long as, it takes place for the sole purpose of carrying out the transmission in the communication network and provided that the information is not stored for a period longer than is reasonably necessary for the transmission to take place.[1308] The provider must not be the one to initiate the transmission, it must not select the receiver of the transmission and it does not select or modify the information contained in the transmission.

Although the second rule is similar to the first, the liability involved greatly differs.[1309] In this instance, the service provider shall not be liable for damages for the automatic, intermediate and temporary storage of that information. However, this must be performed for the sole purpose of making more efficient the information's onward transmission, to other recipients of the service upon their request. The law lays down a set of actions which the provider must have not carried out in order to benefit from the protection against liability. First and foremost, the provider does not modify the information. Secondly, the provider

[1307] Article 19, Electronic Commerce Act, Chapter 426 of the Laws of Malta.
[1308] Article 19(2), Electronic Commerce Act, Chapter 426 of the Laws of Malta.
[1309] Article 20, Electronic Commerce Act, Chapter 426, Laws of Malta.

complies with the conditions to access to the information. Furthermore, the provider adheres to any conditions regulating the updating of the information. They must also not interfere with the technology used to obtain data on the use of the information. Lastly, the provider acts expeditiously to remove or to bar access to the information upon obtaining actual knowledge. This awareness is that the information at the initial source of the transmission has been removed from the network, or access to the information has been barred, or the Court or competent regulator has ordered the removal or barring of access to the information. [1310]

The final rule is that governing special liability involves hosting service providers,[1311] whereby the information society service is provided, and consists of the storage of information, which is provided by the recipient of that service, who must also not be acting under the authority or control of the service provider. The latter is not liable for damages for the information stored at the request of a recipient of the service. However, this exemption from liability is dependent on either of the following two circumstances: the provider of the service does not have the actual knowledge that the activity is illegal and is not aware of the facts or circumstances from which illegal is evident, or, upon obtaining such knowledge or awareness that the act is illegal, he acts expeditiously to remove or disable access to the aforementioned information.

It can be deduced that liability of intermediary service providers would arise where ISPs fail to act in the manner laid down in the Electronic Commerce Act, which will not provide them with the necessary defence against liability.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will most likely face a future of stricter clampdowns. This is so due to the digital age that the world finds itself in, which boasts numerous advantages but is not short of its disadvantages either. It aids in promoting the right to freedom of expression and provides a platform for one to exercise this right. However, this freedom to express, which is highly valued by many, allows room for one to misuse and abuse this right.

[1310] Article 20, ibid.
[1311] Article 21, ibid.

This calls for legislation to be put into place to fight crime and protect citizens which will in turn pose the undesired effect of the restriction and infringement of one's rights, particularly the right to freedom of expression. A latest example of the unsettling rise of internet censorship in Europe is the approval of the controversial EU Copyright Directive which seeks to enhance the rights for copyright owners but at the cost of internet freedom. This may provide a clear picture of the direction that legislators intend to follow when it comes to internet censorship, which calls for the need to strike a balance between safeguarding and surveillance on the internet.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

Article 11 of the EU charter of Human Rights states that 'Everyone has the right to freedom of expression', this in turn includes the right to share and hold opinions without prejudice of public interference, irrespective of any standing frontiers. This Article also holds that freedom of the media shall be respected and that they shall have a right to operate within the jurisdiction of the signatory states without interference or influence from third parties. Malta, as a signatory and member of the European Union, also holds and has ratified such Article and so Maltese Law on Freedom of Expression is mainly based on this charter, since this has taken precedence over any preceding law in place. Further clarification on the freedom of expression in Malta can be found in Article 41 of the Constitution, where the legislator sought to further solidify Malta's position on freedom of speech by firstly establishing that Article 11 of the European Charter is to be followed and that no law may be promulgated against. It also goes on to establish the instances where the freedom of expression in the country may be limited due to the protection of people's rights or the state's security.

Due to the recent death of the journalist Daphne Caruana Galizia, the ongoing court case of Malta's laws on freedom of expression as well as hate speech, have been put under scrutiny, both by the Maltese people themselves and by other states and institutions such as the European Union. As can be seen from the study conducted by the World Bank, which looks into the freedom of expression and accountability of over 200 countries, Malta's standing on free speech is quite negative compared to other countries included in this study. By using Worldwide

Governance Indicators, the results of this study have indicated that the citizens of Malta have found it difficult to participate in selecting their government, expressing their opinion and having adequate access to freedom of association and media. Having ranked at its lowest, being 87.2% in 2017, the last year in which the study was conducted, this ranking is only expected to be lowered after the recent events that took place in the country.[1312]

On the other hand, in order to protect its citizens from hate speech and harmful altercations online, Maltese legislation does provide a number of legal remedies in its Criminal Code. Article 82A(1) of this code, primarily defines hate speech as: 'Whosoever uses any threatening, abusive or insulting words or behaviour, or displays any written or printed material which is threatening, abusive or insulting, or otherwise conducts himself in such a manner, with intent thereby to stir up violence or racial or religious hatred against another person or group on the grounds of gender, gender identity, sexual orientation, race, colour, language, ethnic origin, religion or belief or political or other opinion or whereby such violence or racial or religious hatred is likely, having regard to all the circumstances, to be stirred up shall, on conviction, be liable to imprisonment for a term from 6 to 18 months.'

This article clearly shows the legislator's intention to offer protection and to prevent vehemence against the dignity of the people who are victim to this crime, rather than limiting the freedom of expression of those who choose to use insulting or negative behaviour towards others online. In the case of Police vs Norman Lowell (2013), Mr. Lowell was charged with the crime of incitement of violence and hatred, due to the comments he made towards irregular immigrants and citizens of a foreign nationality in Malta, particularly during the three political meetings that he organised in order to promote his own political party. Upon appearing before the criminal court, the honourable judge Lawrence Quintano, stated that Article 82A constitutes within it both the *actus reus* and the *mens rea* and held that the tonality and vocabulary used by Mr. Lowell were such that they convey his intention to cause harm. The fact that such harmful words were uploaded onto Lowell's website was taken into account by the court, as this aided in creating more harm to the public since it made it easily accessible to anyone browsing the internet. Furthermore, Judge Quintano also addressed the issue of freedom of speech and stated that freedom of expression, which is a right that every human being has, is impinged on when statements become racist

[1312] Claire Caruana, 'Freedom Of Expression, Free Media In Malta Rank Lowest In 10 Years, Times of Malta (2018) <https://timesofmalta.com/articles/view/freedom-of-expression-free-media-in-malta-rank-lowest-in-10-years.690857> accessed 23 February 2020.

and harmful to others. In order to further strengthen his position on this, the judge also delved into previous cases of hate speech that took place in Malta in the previous years.[1313]

In addition to the legislation present in the Criminal Code, on the 24 May 2018 Malta also replaced the Press Act with the Media and Defamation Act which had been in place in the previous years. This act seeks to address issues such as defamation, libel, and slander present in the media whilst the Press Act only addressed these issues when they were present on 'written media'. In order to protect the rights of civilians, the legislator here made the right decision to further enact laws to prevent issues that are occurring in the modern-day world. This was a necessary change for Malta in order to protect the Rights of its citizens.[1314]

This new legislation seeks to prevent defamation against defamatory statements. In this case, the plaintiff is bound with the onus of proof to show that serious harm has ensued or is likely to ensue from such statements. The plaintiff also has the right to prove that the imputations against him can seriously harm his reputation or cause damage to his credibility.

On the other hand, one of the most important additions in this new act is the balance between the protection of private life and what is of public interest. Article 4(5) of the Media and Defamation Act precludes the defence of the truth if the matters at hand are considered to be the private life of the plaintiff and if the allegations do not hinder the plaintiff's exercise of his public functions or possession of trade. The court has been given great discretion in the proceedings brought before it regarding this act, especially in cases where the defence raised is that that a matter is of public opinion or general public interest. This act also gives the court discretion in in matters where the plaintiff is involved in matters public interest as well as where the court deems it necessary that raising such a defence is crucial for the proper administration of justice.[1315]

A significant change that the Media and Defamation Act brought about is that Article 9 holds that the Court of Justice is now able to award moral damages in addition to financial payments for the material damages done. This is a great steppingstone towards the protection against hate speech as now, those found guilty of slander may be fined an extra sum of up to €5000 for moral damages.[1316]

[1313] Police vs Norman Lowell [2013] Court of Criminal Appeal, Criminal Appeal Number 98/2011.

[1314] The Media And Defamation Act, 2018 - Iuris Malta (Iuris Malta, 2018) <http://iurismalta.com/media-defamation-act-2018/> accessed 23 February 2020.

[1315] Police vs Norman Lowell [2013] Court of Criminal Appeal, Criminal Appeal Number 98/2011.

[1316] The Media And Defamation Act, 2018 - Iuris Malta (Iuris Malta, 2018) <http://iurismalta.com/media-defamation-act-2018/> accessed 23 February 2020.

In conclusion, it is opined that although Malta's position regarding freedom of expression online could be improved, actions are being taken to improve the country's democracy and moreover, prevention methods that hinder this from succeeding are being put in place. It is ultimately the responsibility of governmental bodies and the Court of Justice to ensure that the system of cheques and balances set up is applied properly and that nothing hinders the application of the Rule of Law in the country.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

Malta, as a country that is a signatory of the European Union has a duty to respect Human Rights and abide by the laws set by the Union regarding such a matter. The European Union has the right to intervene where it deems fit or where matters are brought up before its Court or its Ombudsman in relation to the observance of Human Rights. Furthermore, the 1959 Convention ensured further protection of these rights since Malta's Constitution is absolute and no law may be ratified against any law present within it. As a democratic country, Malta holds within it the Right to Freedom of Expression, which must also be observed on online platforms.

Having said that, in order to ensure that people's rights are protected and that there is a respect towards others online, the legislation in place also mentions instances where freedom of expression may be limited. The Media and Defamation Act (2018) was specifically enacted to ensure that both the public and the media are protected when the public uses technological media to express its opinion.

Apart from this, in order to establish the limitation of freedom of expression online, the Maltese Courts shall, on a case by case basis, apply a three-part test that was established by the European Union. This test takes into consideration and allows for freedom of speech to be limited where, firstly, the interference is promulgated in the country's domestic laws. Additionally, the interference is necessary for a domestic society to function harmoniously. It is also limited to protect the interest of national security, to prevent disorder and harm, to protect

morals and the reputation of others, to protect health, to protect information given in confidence, in order to maintain the impartiality of the Court.[1317]

Thus, Malta has established a balance between Freedom of expression and the protection of human rights doubly. Firstly, the Convention has recognised Human Rights and therefore ensures that each and every one of these Human Rights are protected by the laws promulgated within it. Secondly, since Malta is a member of the European Union, any person both Maltese or foreign is also protected by the legislation of the European Union. Any person who feels that their rights have been impinged upon may appeal in front of the Courts, and the judiciary who is fair and impartial may rule on their allegation. If no remedy is found in the domestic courts, individuals also have the right to appeal in front of the European Court of Human Rights which is considered to be the highest Court to preside over a Human Rights matter.

In this sense, it cannot be said that Malta has reached a balance between the protection of Human Rights and the protection of free speech online. Malta's legislation has been amended to recognise that this right also exists online, and measures have been taken to ensure that this is respected without impeding on the basic rights of others. Damages will be awarded by the court where deemed necessary in order to justly make good to those who have been wronged by the actions and words of others.

10. How do you rank the access to freedom of expression online in your country?

The online world, which has developed rapidly over recent years since it was created in 1983, has become widespread to the point of having access to it from every home and jeans-pocket all around the world. Technology has surpassed all its original limited functions becoming increasingly advanced with every year that goes by, however, its original function of transmitting information from one place to another has been sustained.

Keeping in mind such an easy access to information, some of it may be regarded to be sensitive and thus, certain parties might want to be control it. This is leading and will lead to online censorship which, in the physical world, would be a breach to the right of freedom of speech as established, for example, by the 'Charter of Fundamental Rights of the European Union'. Article 11 which was

[1317] Dominika Bychawska-Siniarska, 'Protecting The Rights To Freedom Of Expression Under The European Convention Of Human Rights' (Council of Europe 2017) <https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814> accessed 23 February 2020.

signed by Malta through its accession to the European Union in 2004, states the following '1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.'

A healthy practice within the day-to-day operation of a democracy is said to be that of criticism. Criticism offers a challenge to power and also acts against the abuse of such power. Very often, such criticism is published through the use of the media of the country like newspapers, journals, and articles which can be either of a physical nature or nowadays, with the widespread use of technology, can be found online.

The limitation of criticism, usually aimed towards the government by various means of censorship, is a popular tool used by dictatorships to quell opposition. As an example, this can be seen through the People's Republic of China's setting up of the Great Firewall of China. This seeks to regulate the use of the internet internally from foreign websites, earning it the nickname of '*qiangguo',* meaning 'wall nation'.[1318] North Korea is another nation which keeps a tight grip on censorship of the media where all media outlets are controlled and owned by the government. The radios found in North Korea only receive government frequencies and contain a seal to prevent tampering.

Like in many other countries, Malta is facing the new wave of SLAPP (Strategic Lawsuits against Public Participation) cases due to individuals who participate actively in making use of their Right of online Freedom of Expression such as journalists and bloggers.

George W. Pring states that 'SLAPPs raise substantial concern for the future of citizen involvement or public participation in government'.[1319] Popular cases of SLAPP in Malta include Satabank filing lawsuit cases in Bulgaria against Maltese journalist Manuel Delia for money laundering accusations, and the case of the journalistic website 'The Shift' threatened to be sued by Henley and Partners – a British company employed by the Maltese government to take care of the passport scheme and which was believed to have been involved in a scandal in Grenada. Matthew Caruana Galizia even described having a SLAPP cripple

[1318] Elizabeth C Economy 'The Great Firewall of China: Xi Jinping's Internet Shutdown' (The Guardian, 29 June 2018) <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown> accessed 20 February 2020.

[1319] George W. Pring, 'SLAPPs: Strategic Lawsuits against Public Participation', (1989) 7(11) Pace Environmental Law Review <https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1535&context=pelr> accessed 20 February 2020.

one's freedom of expression as a form of 'torture'.[1320] Above all, this effectively results in a form of censorship, taking away the freedom of expression that everyone is entitled to, not by legal injunction but by demoralising and depoliticising. Caruana Galizia's mother, the late journalist Daphne Caruana Galizia, who had numerous libel cases against powerful politicians and companies, was brutally murdered by way of car bombing in October 2017, and this can be interpreted as the ultimate form of censorship.

As with all things, such freedom, especially a faceless and anonymous one, brings about abuse, both from the user and from the persons in charge to moderate it. As of recently, hate speech has shown to be more frequent on the internet over the past years as it tends to attract attention. This is a dangerous practice as the internet is a level playing field that is available for everyone to see, including children and young adults who are still forming their opinions on certain matters and thus considered impressionable. Such hate speech may even have a negative effect in real life and cause certain events. This came out clearly when in April of 2018 two soldiers from the Armed Forces of Malta, aged 21 and 22 years of age, were accused of having shot Lassana Cisse Souleymane, 42, from the Ivory Coast in a racially-motivated drive-by shooting in Hal Far.[1321] Prosecutors insist that the man had been shot because of the colour of his skin. The two soldiers are also accused with the attempted murder, from which grievous bodily harm ensued, of two migrants from Gambia on the same night. This event occurred after an increase in a string of racially abusive posts, and comments appeared more frequently, *ad hominem,* on the internet on Maltese websites prior to such incident.

In her writing 'Understanding Hate Speech',[1322] Sandy Starr says that 'The Internet is a distorted reflection of society, where minority and extreme opinion are indistinguishable from the mainstream'. This therefore goes to show that Malta does struggle with certain issues relating to freedom of expression. Access to freedom of expression online does not seem to be the problem, like in other previously mentioned dictatorships where censorship is enforced. At face value Malta seems to be quite liberal, however when it comes to criticism often involving public action, people such as journalists, bloggers, or the average users

[1320] The Shift Team, 'Opposition files Bill to protect journalists from SLAPP, again' (The Shift News, February 2020) <https://theshiftnews.com/2020/02/27/opposition-files-bill-to-protect-journalists-from-slapp-suits-again/> accessed 20 February 2020.

[1321] Matthew Agius 'Looking back at 2019 - So much Crime so Little Time' (maltatoday, 2 January 2020) <https://www.maltatoday.com.mt/news/court_and_police/99470/looking_back_at_2019_so_much_crime_so_little_time#.XlD1CEoo82w> accessed 20 February 2020.

[1322] Sandy Starr, 'Hate Speech on the Internet' <https://www.osce.org/fom/13846?download=true> accessed 20 February 2020.

of online platforms might encounter certain difficulties to maintain their freedom of expression. This is seen through libel and SLAPP cases which could ultimately incur fiscal punishments and risk the article or blog being taken down. The Party in Opposition in the parliament of Malta, in February 2020 proposed a draft legislation to the Parliament of Malta to **'**protect Maltese journalists from expensive and long-drawn-out strategic lawsuits of public participation (SLAPP) filed against them in different countries, safeguarding media freedom'.[1323] This, however, failed in April 2018 due to the government voting against it.

Hence, although censorship is not enforced, further legislation appears to be needed to guarantee that the freedom of expression online acts as a protection for those who participate and criticise shortcomings or abuses of power. Apart from this, other legislation seems to be needed to control the rise of Hate Speech in Malta to prevent the depravation of other rights such as the fundamental human right to life.

11. How do you overall assess the legal situation in your country regarding internet censorship?

Laws are by nature a dynamic notion; they are a reflection of the culture's values which consequently change and alter over time, and thus, because of this, laws change and adapt too. If laws remain sedentary, they become obsolete, especially with the pace at which society is changing in the present day. In the world of technology and the internet this change seems to be moving the fastest, and legislation must keep up for the ever-growing need for regulation of abuse.

Malta's journey has been one of great progress from a time when censorship was strict under the British to the granting of freedom of the press in 1839 which later evolved into the laws, we have today which protect the freedom of expression and publication.[1324]

Legislatively, Malta has set up a legal framework which seeks to protect the rights of a legal person. The rights of a person are enshrined within Chapter IV of the Constitution of Malta 'Fundamental Rights and Freedoms of the Individual', in Articles 32 and 47.

[1323] The Shift Team, 'Opposition files Bill to protect journalists from SLAPP, again' (The Shift News, February 2020) <https://theshiftnews.com/2020/02/27/opposition-files-bill-to-protect-journalists-from-slapp-suits-again/> accessed 20 February 2020.

[1324] Henry Frendo, 'Maltese Journalism, 1838-1992 : An Historical Overview' (Press Club Malta 1994),

Most relevant to our discussion is that the Constitution of Malta, within the aforementioned Chapter IV, lists under Article 41 the 'Protection of Freedom of Expression'.

Sub-Articles 2 to 5 go on to list the exceptions to when interference of such publications and impediment of freedom of expressions are allowed. These include 'the interests of defence, public safety, public order, public morality or decency, or public health;' as can be found under sub-Article 2(a)(i). It can also be the case that freedom of expression is denied as it may breach other fundamental human rights as stated in sub-Article 2(a)(ii).

Malta has taken a more liberal stance in certain areas over the past years as is in the regard of the vilification of religion, for example. This vilification of all religions in Malta in 2016, formerly Article 163 and 164 of the Criminal Code, shocked the religious communities in Malta. The response of such communities was that the repealing of such laws was too liberal, however as a result, freedom of expression in Malta can be, objectively, considered to be wider.

Since the online platform for posting and sharing opinions is a relatively new one, regulation of it is still in the development stage to prevent abuses such as the new wave of hate speech online. Nonetheless, Malta is updating its laws to cater for this change. Updates in the legislation can be seen in the changing of the Maltese Press Act. As stated in other sections, this act was repealed and was replaced by the Media and Defamation Act (Cap. 579 of the Laws of Malta).

As previously mentioned, the fact that people may write freely and even anonymously online has given rise to abuse, in particular, when it comes to long-harboured sentiments of resent that may not be socially acceptable when spoken. These therefore manifest in the form of hate speech online and this has developed into a problem which caught the attention of the government after some alarming statistics.

In October of 2019 the Maltese government founded a new Hate Speech and Crime Unit under the Home Affairs Minister, Michael Farrugia. The project is financed by the European Union in partnership with the Ministry for Home Affairs and National Security, the Malta Police Force, the Academy for Disciplined Forces, the Agency for Protection of Persons Seeking Asylum (AWAS), the Director for Integration and Equality, the Commission for the Rights of Disabled Persons, and the Victims Support Europe.[1325] The aid offered will be both of a therapeutic nature and a legal one. A poll in 2016 by SOS Malta

[1325] New Crime and Speech Unit inaugurated' (independent.com.mt. 2019) <https://www.independent.com.mt/articles/2019-10-24/local-news/New-Hate-Crime-and-Speech-Unit-inaugurated-6736215235> accessed 20 February 2020.

showed that 34% of its study group had been a victim of hate speech and 8% had been subject to hate crime. The factors contributing to the commission of such hate crimes have also been narrowed down to nationality, political opinion and religion.

Another recurring action that takes places is that of Strategic Lawsuit against Public Participation (SLAPP) which is defined as 'a civil lawsuit brought as an intimidation measure against an activist'.[1326] Here, when companies are criticised by journalists, bloggers, or individuals who have sensitive information, the said company may file a lawsuit against the person criticising with the intention of cutting off their financial means to continue their work. Therefore, this can be seen as a tool of political and legal intimidation, and one may go as far as calling it censorship working within the parameters of the law. An example of this can be seen in the two separate SLAPP lawsuits that the Bulgarian owner of Satabank in Malta filed in a Bulgarian court against the Maltese blogger Manuel Delia and The Times of Malta.[1327] In his blog, Manuel Delia stated 'Satabank was licensed by the Maltese authorities and operated its business between March 2016 until October 2018 when its business was frozen by order of the financial services authority. In 2019 it was fined a record €3 million…'.[1328] Consequently, after such exposition of details, the lawsuits were filed as a means of silencing.

One may however ask whether it is acceptable that power and money can buy silence in this day and age through legal means.

On the other hand, sometimes this freedom of speech online may cause abuse from the point of view of writers: apart from the abuses of the right of freedom of expression, this right is also used as a political tool. It often happens that ordinary citizens or journalists write and post articles about people in authority which at *prima facie* may look shocking and scandalous but would result in having no substantive value; their only intention being that of slander. To counteract this practice, from the earliest of days when freedom of the press was introduced back in 1839, the law of libel has always been active. According to the Merriam-Webster dictionary 'libel' is defined as 'a written or oral defamatory statement or representation that conveys an unjustly unfavourable impression'. This can be seen through cases such as *Farrugia Julia v. Caruana Galizia Daphne*.[1329]

[1326] Dictionary.com 'SLAPP' <https://www.dictionary.com/browse/slapp> accessed 20 February 2020.

[1327] Juan Ameen, 'The Silence behind the SLAPP' (The Shift, March 2020) <https://theshiftnews.com/2020/03/11/the-silence-behind-the-slapp/> accessed 20 February 2020.

[1328] Manuel Delia, 'The Times of Malta also SLAPPed in Bulgara by Satabank owner' (Truth be Told, 27 February 2020) <https://manueldelia.com/2020/02/the-times-of-malta-also-slapped-in-bulgaria-by-satabank-owner/> accessed 28 February 2020.

[1329] Farrugia Julia v Caruana Galizia Daphne [2015], Court of Magistrates (Civil)

It was also such cases of libel that occurred when the nature of the article was considered to be scandalous, and persons open libel cases to try and have the article removed. An example of this can be seen through cases such as *Patrick Dalli v. Caroline Muscat*. As previously mentioned, in order to regulate further this issue of defamation and slander, the Government of Malta formally promulgated the Media and Defamation Act in 2017. In this new act, a legal structure was set up to establish penalties and privileges, for example what happens when for example, a case is opened against an editor.

As quoted by the online journal maltatoday 'Deciding where to draw the line between internet hate and free speech is something that requires constant vigilance'.[1330] Therefore, considering all the factors previously mentioned, through this assessment it can be argued that Malta is quite liberal when it comes to freedom of expression, both online and offline. Unfortunately, however, this lack of restriction on the freedom of expression and the freedom to write what may want without any filtering has, as we have seen, given rise to problems. It can also be argued that this could fuel physical world problems which are manifested and birthed online. Hence, one's freedom of expression being totally unrestricted may not only emanate from Malta's liberal approach; it may also emanate from *lacunas* that may be found when dealing with emerging areas within Maltese legislation, thus calling for further updates and new initiatives to keep the internet as the level-playing field it was originally intended to be.

<https://ecourts.gov.mt/onlineservices/Judgements/Details?JudgementId=0&CaseJudgementId=96906> accessed 20 February 2020.

[1330] 'Hate speech limits freedom of expression' (maltatoday, 27 October 2019) <https://www.maltatoday.com.mt/comment/editorial/98254/freedom_of_expression#.XlJUI0oo82y> accessed 20 February 2020.

Table of legislation

Title of the legal act	Provision text in English language
Constitution of Malta 1964, Article 41	(1) Except with his own consent or by way of parental discipline, no person shall be hindered in the enjoyment of his freedom of expression, including freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his correspondence.
Constitution of Malta 1964, Article 32	Whereas every person in Malta is entitled to the fundamental rights and freedoms of the individual, that is to say, the right, whatever his race, place of origin, political opinions, colour, creed, sex, sexual orientation or gender identity, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely – (a) life, liberty, security of the person, the enjoyment of property and the protection of the law; (b) freedom of conscience, of expression and of peaceful assembly and association; and (c) respect for his private and family life, the subsequent provisions of this Chapter shall have effect for the purpose of affording protection to the aforesaid rights and freedoms, subject to such limitations of that protection as are contained in those provisions being limitations designed to ensure that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest.
Data Protection Act 2018, Article 9	(1) Personal data processed for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes or for the purposes of academic, artistic or literary expression, shall be exempt from compliance with the provisions of the Regulation specified in sub-article (2) where, having regard to the importance of the right of freedom of expression and information in a democratic society, compliance with any of the provisions as specified in sub-article (2) would be incompatible with such processing purposes: Provided that when reconciling the right to the protection of personal data with the right to freedom of expression and information, the controller shall ensure that the processing is proportionate, necessary and justified for reasons of substantial public interest.
Press Act 1974, Article 6	Whosoever, by any means mentioned in article 3, shall threaten, insult, or expose to hatred, persecution or contempt, a person or group of persons because of their gender, gender identity, sexual orientation, race, colour, language, ethnic origin, religion or belief or political or other opinion, disability as defined in article 2of the Equal Opportunities (Persons with Disability) Act, shall be

	liable on conviction to imprisonment for a term not exceeding three months and to a fine (multa).
Media and Defamation Act 2018, Article 22	No court or tribunal established by law shall require an editor, author, publisher or operator of a website to disclose the source of information contained in a newspaper or broadcast or website for which he is responsible unless it is established to the satisfaction of the court or tribunal that such disclosure is necessary in a democratic society in the interests of national security, territorial integrity, public safety, or for the prevention of disorder or crime or for the protection of the interests of justice.
Electronic Commerce Act 2002, Article 19	(1) Where an information society service is provided, and such service consists in the transmission, in a communication network, of information provided by the recipient of the service, or the provision of access to a communication network, the provider of such a service shall not be liable, otherwise than under a prohibitory injunction, for the information transmitted. Provided that such provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. (2) The acts of transmission and of the provision of access referred to in sub article (1) hereof, include the automatic intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
Electronic Commerce Act 2002, Article 20	Where an information society service is provided, and such service consists in the transmission, in a communication network, of information provided by a recipient of the service, the provider of that service shall not be liable for damages for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request. Provided that: (a) the provider does not modify the information; (b) the provider complies with the conditions on access to the information; (c) the provider complies with any conditions regulating the updating of the information; (d) the provider does not interfere with the technology used to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to bar access to the information upon obtaining actual knowledge of any of the following: (i) the information at the initial source of the transmission has been removed from the network; (ii) access to it has been barred;

	(iii) the Court or other competent regulator has ordered such removal or barring.
Electronic Commerce Act 2002, Article 21	(1) Where an information society service is provided, and such service consists in the storage of information provided by a recipient of the service, the provider of that service shall not be liable for damages for the information stored at the request of a recipient of the service. Provided that: (a) the provider does not have actual knowledge that the activity is illegal and is not aware of facts or circumstances from which illegal activity is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. (2) Sub article (1) shall not apply when the recipient of the service is acting under the authority or the control of the provider of the service.
Criminal Code 1854, Article 82A	(1) Whosoever uses any threatening, abusive or insulting words or behaviour, or displays any written or printed material which is threatening, abusive or insulting, or otherwise conducts himself in such a manner, with intent thereby to stir up violence or racial or religious hatred against another person or group on the grounds of gender, gender identity, sexual orientation, race, colour, language, ethnic origin, religion or belief or political or other opinion or whereby such violence or racial or religious hatred is likely, having regard to all the circumstances, to be stirred up shall, on conviction, be liable to imprisonment for a term from six to eighteen months. (2) For the purposes of the foregoing sub-article "violence or racial or religious hatred" means violence or racial or religious hatred against a person or against a group of persons in Malta defined by reference to gender, gender identity, sexual orientation, race, colour, language, national or ethnic origin, citizenship, religion or belief or political or other opinion.
Media and Defamation Act 2018, Article 4(5)	(5) The defences referred to in sub-articles (1) and (2) shall only apply where the person aggrieved is a public figure, such as when the said person: (a) is a public officer or servant or an officer or servant of a body established by law or of a body in which the Government of Malta has a controlling interest; or (b) is a candidate for a public office and the facts attributed to him refer to his honesty, ability or competency to fill that office; or (c) habitually exercises a profession, art or trade, and the facts attributed to him refer to the exercise of such profession, art or trade; or (d) takes an active part in politics and the facts attributed to him refer to his so taking part in politics; or (e) occupies a position of trust in a matter of general public interest: Provided that the truth of the matters charged may not be enquired into if such matters refer to the private life of the

	plaintiff and the facts alleged have no significant bearing on the exercise of the plaintiff's public functions, office, profession or trade: Provided further that, notwithstanding the provisions of this sub-article, the defences referred to in sub-articles (1) and (2) may be raised where the matter referred to is a matter of general public interest or where the person aggrieved, although not being a public figure is involved in matters of public interest or where after giving due consideration to all the circumstances of the claim the Court is satisfied that the raising of the said defences is necessary in the interests of the proper administration of justice.
Media and Defamation Act 2018, Article 9	In proceedings instituted under this Act, the Court may order the defendant to pay a sum not exceeding eleven thousand, six hundred and forty euro (€11,640) by way of moral damages in addition to actual damages under any law for the time being in force: Article
Constitution of Malta 1964, Article 41	(1) Except with his own consent or by way of parental discipline, no person shall be hindered in the enjoyment of his freedom of expression, including freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference (whether the communication be to the public generally or to any person or class of persons) and freedom from interference with his correspondence. (2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of sub-article (1) of this article to the extent that the law in question makes provision – (a) that is reasonably required – (i) in the interests of defence, public safety, public order, public morality or decency, or public health; or (ii) for the purpose of protecting the reputations, rights and freedoms of other persons, or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts, protecting the privileges of Parliament, or regulating telephony, telegraphy, posts, wireless broadcasting, television or other means of communication, public exhibitions or public entertainments; or (b) that imposes restrictions upon public officers, and except so far as that provision or, as the case may be, the thing done under the authority thereof is shown not to be reasonably justifiable in a democratic society. (3) Anyone who is resident in Malta may edit or print a newspaper or journal published daily or periodically: Provided that provision may be made by law - (a) prohibiting or restricting the editing or printing of any such newspaper or journal by persons under twenty-one years of age; and (b) requiring any person who is the editor or printer of any such newspaper or journal to inform the prescribed authority to that

	effect and of his age and to keep the prescribed authority informed of his place of residence. (4) Where the police seize any edition of a newspaper as being the means whereby a criminal offence has been committed they shall within twenty-four hours of the seizure bring the seizure to the notice of the competent court and if the court is not satisfied that there is a prima facie case of such offence, that edition shall be returned to the person from whom it was seized. (5) No person shall be deprived of his citizenship under any provisions made under article 30(1) (b) of this Constitution or of his juridical capacity by reason only of his political opinions.
Media and Defamation Act 2018, Article 12	(1) This article applies where an action for defamation is brought against the editor of a website in respect of a statement posted on the website. (2) It is a defence in mitigation of damages for the editor to show that it was not the operator or person who posted the statement on the website. (3) The defence is defeated if the plaintiff shows that – (a) it was not possible for the plaintiff to identify the person who posted the statement, and (b) the plaintiff gave the editor a notice of complaint in relation to the statement, and (c) the editor failed to respond to the notice of complaint or did not act in accordance with any provision contained in regulations about such notices. (4) For the purposes of paragraph (a) of sub-article (3), it is possible for a claimant to "identify" a person only if the claimant has sufficient information to bring proceedings against the person. (5) The Minister may by regulations which shall be made after a consultation process, and which shall take into account the need to guarantee a fair balance between the protection reputation of persons and freedom of expression exercised as is necessary in a democratic society, and which shall be approved by resolution of the House of Representatives before they come into force: (a) make provision as to the action required to be taken by an editor of a website in response to a notice of complaint which may in particular include action relating to the identity or contact details of the person who posted the statement and action relating to its removal; (b) make provision specifying a time limit for the taking of any such action; (c) make any other provision for the purposes of this article. (6) Subject to any provision made by virtue of sub-article (5), a notice of complaint is a notice which – (a) specifies the complainant's name, (b) sets out the statement concerned and explains why it is defamatory of the complainant, (c) specifies where on the website the statement was posted, and (d) contains such other information as may be specified in regulations.

	(7) The defence under this article is defeated if the plaintiff shows that the editor of the website has acted with malice in relation to the posting of the statement concerned. (8) The defence under this article is not defeated by reason only of the fact that the editor of the website moderates the statements posted on it by others.
General Data Protection Regulations (EU Directive 2016/679) 2016, Regulation 85	1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. 2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information. 3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.
General Data Protection Regulations (EU Directive 2016/679) 2016, Regulation 17	1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; c. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); d. the personal data have been unlawfully processed; e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by

	such controllers of any links to, or copy or replication of, those personal data. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: a. for exercising the right of freedom of expression and information; b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or e. for the establishment, exercise or defence of legal claims.
Charter of Fundamental Rights of the European Union 2000, Article 11	1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.
Universal Declaration of Human Rights 1948, Article 19	Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Bibliography

English titles

Legislation

Charter of Fundamental Rights of the European Union 2000

Council Regulation (EC) 2016/679 of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data And Repealing Directive 95/46/EC [2016] OJ L119/1.

European Convention on Human Rights 1953

Universal Declaration of Human Rights 1948

Periodicals

Pring G., 'SLAPPs: Strategic Lawsuits against Public Participation', Pace Environmental Law Review (1989) Volume 7 Issue 11.

Digital resources

'The Silence behind the SLAPP' <https://theshiftnews.com/2020/03/11/the-silence-behind-the-slapp/> accessed 10th April 2020

Economy E, 'The Great Firewall Of China: Xi Jinping's Internet Shutdown' <https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown>

Starr S, 'Hate Speech on the Internet' <https://www.osce.org/fom/13846?download=true>

The Shift Team, 'Opposition files bill to protect journalists from SLAPP suits, again' <https://theshiftnews.com/2020/02/27/opposition-files-bill-to-protect-journalists-from-slapp-suits-again/> accessed 12th April 2020

Maltese titles

Legislation

Act No. XI, 2018, Laws of Malta

Constitution of Malta, Laws of Malta

Criminal Code, Chapter 9, Laws of Malta

Data Protection Act, Chapter 586, Laws of Malta

Media and Defamation Act, Chapter 579, Laws of Malta

Press Act, Chapter 248, Laws of Malta

Books

Borg T, Commentary On The Constitution Of Malta (Kite Group 2016)

Frendo H, 'Maltese Journalism, 1838-1992 : An Historical Overview' (Press Club Malta 1994)

Gatt K, 'Hate Speech And The Freedom Of Expression - Is The Legislation Of The High Contracting Parties In Line With ECHR Principles?' (Doctor of Laws (LLD), University of Malta 2017)

Digital resources

'New Hate Crime and Speech Unit Inaugurated' <https://www.independent.com.mt/articles/2019-10-24/local-news/New-Hate-Crime-and-Speech-Unit-inaugurated-6736215235>

'Criminal Libel Is History As New Media Law Comes Into Force' (Times of Malta, 2020) <https://timesofmalta.com/articles/view/criminal-libel-is-history-as-new-media-law-comes-into-force.679111>

'Data Protection: EU Citizens' Right To Be Forgotten Limited To EU Territory - Iuris Malta' (*Iuris Malta*, 2020) <http://iurismalta.com/data-protection-eu-citizens-right-forgotten-limited-eu-territory/>

Hate Speech Limits Freedom of Expression <https://www.maltatoday.com.mt/comment/editorial/98254/freedom_of_expression#.XlJUI0oo82y>

'The Media And Defamation Act, 2018 - Iuris Malta' (*Iuris Malta*, 2018) <http://iurismalta.com/media-defamation-act-2018/>

Agius M, 'Looking Back at 2019: So much crime, so little time' <https://www.maltatoday.com.mt/news/court_and_police/99470/looking_back_at_2019_so_much_crime_so_little_time#.XlD1CEoo82w>
Caruana C, 'Freedom Of Expression, Free Media In Malta Rank Lowest In 10 Years' (Times of Malta 2018) <https://timesofmalta.com/articles/view/freedom-of-expression-free-media-in-malta-rank-lowest-in-10-years.690857>

Delia M, 'The Times Of Malta also SLAPPed in Bulgaria by Satana Bank Owner' <https://manueldelia.com/2020/02/the-times-of-malta-also-slapped-in-bulgaria-by-satabank-owner/> accessed 11th April 2020

Galea A, 'Court Judgments Removed From Internet: Right To Be Forgotten Must Be Respected – Bonnici - The Malta Independent' (Independent.com.mt, 2020) <https://www.independent.com.mt/articles/2019-05-17/local-news/Court-judgments-removed-from-internet-Right-to-be-forgotten-must-be-respected-Bonnici-6736208252>

Vella M, 'Erasing The Right To Know: Maltese Courts Applying Restrictive Interpretation Of Privacy Rules' (MaltaToday.com.mt, 2020) <https://www.maltatoday.com.mt/news/national/86330/erasing_the_right_to_know_maltese_courts_applying_restrictive_interpretation_of_privacy_rules#.XkftVS3MxQI>

Case law

Farrugia Julia v Caruana Galizia Daphne [2015] Court of Magistrates (Civil) Reference 46/2011

Police vs Massimo Gorla [1986] Constitutional Court

Police vs Norman Lowell [2013] Court of Criminal Appeal, Criminal Appeal Number 98/2011

ELSA the Netherlands

Contributors

National Coordinator

Gabrielė Vilemo Gotkovič

National Researchers

Armintė Lydekaitė

Diana Bernardini

Kateryna Nosenko

Kirill Ryabtsev

Lencia Leslie

Livija Šepetytė

Lucas Dikkers

Mădălina Nicolai

Maxim Cassiers

National Linguistic Editors

Hannah Kuzee

Saskia Forman

National Technical Editor

Giulia Carraro

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

1.1. The Basics of freedom of expression

Nowadays, freedom of expression is gaining more momentum than ever as a result of the popularity of different platforms of communication, both online and offline. The exercise of the Freedom of Expression is imperative to a well-functioning democratic society and can be considered a general backbone for the exchange of ideas between individuals. The protection of the principle of the Freedom of Expression is codified in a plurality of international legislative documents, one of them being the Universal Declaration of Human Rights. Not only is the principle important between individuals, it also acts as a way to ensure that the government does not abuse their powers by requiring that the media is independent and non-partisan. The independent media is for that reason one of the most important subcategories of the freedom of expression. The freedom is an important aspect in communication between the public and the government as it allows the general public to have a secure platform for their opinions and views without government interference. With the freedom of expression, individuals can also vocalise information about the violation of other human rights - or the possibility thereof - making it an indispensable freedom when it comes to the protection of human rights. As a result, the importance of the guarantee for the enjoyment of freedom of expression is undeniable.

1.2. Protection

The Dutch government is internationally known to be a tolerant, progressive and democratic State. The government actively encourages these views by being a signatory party to many international human rights agreements, most of which stem from the aforementioned Universal Declaration of Human Rights.[1331]

The Dutch Constitution and other legislation guarantee fundamental freedoms and tend to prioritise tolerance and acceptance in all aspects of society, which allows the Dutch citizens to enjoy a comparatively higher protection of personal rights and freedoms in relation to other countries. The Freedom of Expression is protected in the Dutch Constitution under Article 7. However, it is important to note that there is no explicit mention of the 'freedom of expression' as such, whereas it is explicitly stated in that exact phrasing in the international documents. Instead, the article focuses on the freedom of press and the freedom

[1331] Human Rights In The Netherlands (Government.nl) <https://www.government.nl/topics/human-rights/human-rights-in-the-netherlands> accessed 18 January 2020.

of advertising. With free media being one of the core aspects of the freedom of expression, the Dutch Association of Journalists enjoys significant leeway on the content that can be published. As a result, the Netherlands is known as having one of the least restricted forms of press in the world.[1332] In addition to the freedom of press being a constitutional right, the Dutch government shows their drive for freedom by playing an important role in the Freedom Online Coalition, which is a coalition that aims to achieve absolute Freedom of Expression in international organisations such as the Council of Europe, the Organisation for Security and Cooperation in Europe (OSCE) and many others.

The lack of restrictions on the freedom of speech and expression is considered to be one of the fundamental pillars of the progressive society of the Netherlands given that it means that Dutch citizens can voice their concerns and freely discuss potentially controversial matters. This can be exemplified by the fact that the Dutch government pledged in 2011 to spend six million euros on the promotion of the freedom of expression, which was also to include a portion for bloggers and activists in states where the Freedom of Expression is not as protected as it is in the Netherlands.[1333] Not only is this an issue recognised by the Dutch government, but the Freedom of Expression is also recognised and protected by the European Union as one of the fundamental rights.[1334]

1.3. Hate speech

However much one would like to guarantee the complete freedom of expression, one has to take other rights into consideration; one must consider that it may be necessary to restrict the freedom of speech where a person exercises this right and it leads to an interference with the fundamental rights of another individual. The Netherlands has to take this balancing exercise into consideration but has failed to provide a consistent interpretation of limitations to the protection of Freedom of Expression which has resulted in various controversial cases.

The Netherlands has a *lèse majesté* law which entails that insulting the royalty is still a criminal offence. Even though the possible fines for this crime were recently reduced in addition to the reduction of five years to four months

1332 Freedom Of The Press 2017: Netherlands (Freedom House 2017) <https://freedomhouse.org/report/freedom-press/2017/netherlands> accessed 18 January 2020.

1333 'Coalition Of Countries For Free Internet' (Government.nl, 2011) <https://www.government.nl/latest/news/2011/12/14/coalition-of-countries-for-free-internet> accessed 18 January 2020.

1334 Council of Europe, 'Comparative Study On Blocking, Filtering And Take-Down Of Illegal Internet Content' (Council of Europe 2017) page14-19.

imprisonment,[1335] the existence of this type of law is a heavily debated topic in the Netherlands. As recently as January 2020, an individual received 40 hours of community service for insulting Queen Maxima.[1336] However, the King made a statement that he is not authorised to comment on whether he can be insulted or not, as it is a political matter which he cannot reflect upon.[1337] Currently, insulting the royal family is considered a similar offense to insulting a police officer or other civil servant as it is enshrined in the Dutch Criminal Code.[1338]

Moreover, recent developments showcase a firm movement towards a more regulated Freedom of Expression as hate speech has been criminalised. In the Criminal Code of the Netherlands, intentional insults - verbal, written or illustrated - regarding a person's attributes, such as race, sexual orientation and other factors are considered a punishable offence.[1339] One of the most prominent and well-known cases where the legislation regarding hate speech was on the forefront of the debate was in a case in which one of the parties was a member of a right-wing populist political party called the Party for the Freedom (*Partij voor de Vrijheid) (PVV)*. The concerned individual was Geert Wilders, who also happened to be the person to establish the party in 2006. At first the issue not only related to him as an individual, but rather to the party as a whole given that they were considered to promote anti-immigrant and anti-Islamic sentiments through the abuse of the freedom of expression, which in turn – at least in this case – undermines other fundamental principles such as the principle of freedom of religion. Even though Wilders was a politician at the time and enjoyed parliamentary immunity,[1340] the immunity only applies during a parliamentary debate. Since the statements referred to in the case were delivered in a political rally and not a parliamentary debate, the PVV leader was eligible to be tried in a criminal case. This led to Wilders ultimately being convicted for hate speech towards the Moroccan population in the Netherlands.[1341] This was the first Dutch court case where there was a judgement on the basis of hate speech in the Netherlands. As a result, this case also established a precedent when it

1335 Christopher Schuetze, Dutch Parliament Reduces Penalties For Insulting King (The Sydney Morning Herald, 2018) <https://www.smh.com.au/world/europe/dutch-parliament-reduces-penalties-for-insulting-king-20180411-p4z8yx.html> accessed 18 January 2020.

1336 'Taakstraf Voor Beledigen Koningin Maxima' (Rechtspraak.nl, 2020) <https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Midden-Nederland/Nieuws/Paginas/Taakstraf-voor-beledigen-koningin-Maxima.aspx?pk_campaign=rssfeed&pk_medium=rssfeed&> accessed 18 January 2020.

1337 Shandra Martinez, Dutch King: Should Insulting Him Be A Crime? (mlive, 2019) <https://www.mlive.com/business/west-michigan/2015/05/dutch_king_should_insulting_hi.html> accessed 18 January 2020.

1338 Article 267 van de Wetboek van Strafrecht van 3 maart 1881 (Sr).

1339 Arts. 137(c), 137(d) van de Wetboek van Strafrecht van 3 maart 1881 (Sr).

1340 Art 71 Grondwet.

1341 RBSGR (Rechtbank 's-Gravenhage) 09-12-2016 ECLI:NL:RBDHA: 2016:150 14 [online].

comes to the limitation of the Freedom of Expression if it interferes with others' rights and freedoms - more particularly the freedom of religion. In addition, it shows that the Dutch court is willing to put aside parliamentary immunity and restrict the Freedom of Expression in order to uphold the prohibition on hate speech. However, the case has also sparked a debate on whether certain freedoms should be considered more important than others; certain individuals believe that in a progressive state like the Netherlands, particular rights and freedoms - especially the Freedom of Expression - should be more paramount than others.[1342]

1.4. Censorship

Simply put, the essence of the Freedom of Expression is the states' governments being prohibited from restricting individuals from expressing their thoughts. However, complete Freedom of Expression is hard to achieve. When it comes to censorship, the Dutch government does not impose restrictions on online content, which can be seen in Article 7 of the Dutch Constitution. In fact, the Netherlands leaves it up to the courts to rule on limitations of the internet rather than enacting internet-specific legislation.[1343] One of the very few cases where the government did impose restrictions on online content was where it was required that internet providers block a website in 2012 when a torrent site, Pirate Bay, was ruled to infringe copyright. This was later confirmed to be lawful by the Dutch Court.[1344]

When it comes to the freedom of the press, journalists exercise self-censorship on sensitive topics such as religion. Prior to 2004, journalists did not feel the need to exercise restraint in what they published, but after the murder of a controversial filmmaker, Theo van Gogh, in 2004 journalists have felt the need to be more cautious.[1345] A Dutch Media Authority is nevertheless present and they monitor broadcasters and whether they comply with the Media Act of 2008. However, in order to protect broadcasters from censorship by the government - including the Media Authority itself – the monitoring of programmes only occurs after they have been broadcasted, as the Authority does not have any control over the content itself and cannot prevent something from being

[1342] Jip Stam, 'The Risky Aspects Of Our Hate Speech Laws' (*Leidenlawblog.nl*, 2019) <https://leidenlawblog.nl/articles/the-risky-aspects-of-our-hate-speech-laws> accessed 23 January 2020.

[1343] The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, page14-19.

[1344] RBSGR (Rechtbank 's-Gravenhage) 10-05-2012, ECLI:NL:RBSGR: 2012:BW5387 [online].

[1345] Jason Burke, The Murder That Shattered Holland's Liberal Dream (the Guardian, 2004) <https://www.theguardian.com/world/2004/nov/07/terrorism.religion> accessed 2 February 2020.

broadcasted.[1346] This guarantees that the journalists and broadcasters have the right to censor and restrict themselves as they see fit, which is then checked afterwards if it was done accordingly.

Another aspect in which one can see the lack of Dutch governmental interference in restricting the Freedom of Expression can be seen from the fact that the Dutch government allows the public to view their information.[1347] It is enshrined in the Government Information (Public Access) Act (*Wet openbaarheid van bestuur*) (WOB). The right to information is twofold in the Netherlands: on the one hand, the government actively shares information with the public via campaigns, press conferences and online publications, and on the other hand through passive communication which essentially means allowing individuals to request information from the government. The latter can be exercised by submitting an application for certain data via a variety of government websites. However, it has to be mentioned that there also are limitations to the right to information, namely when the request for information is for confidential data relating to either legal or natural persons - or if it has to be restricted for other security reasons. Moreover, the government retains the right to refuse any application that they consider to be manifestly absurd

1.5. Conclusion

The Freedom of Expression is imperative to states as it allows for individuals in a society to contribute to current discussions and, as a result, to be heard by the government. In addition, it creates a sense of moral equality where everyone's beliefs are as valuable as those of others. Having a discussion on the freedom of expression or a lack thereof is crucial in any state, especially in a nation such as the Netherlands which is well known for its tolerant society and liberal government. As previously stated, the Dutch system is focused on the protection of all constitutional freedoms, including that of the freedom of expression, and it intends to guarantee the highest possible form of protection for these rights. However, this is not always feasible as a balance needs to be stricken between the rights of one individual with the rights of another individual and it cannot always easily be established where to draw the line.

That being said, freedom of expression is protected by the highest law of the state, namely the Constitution. If one were to violate the law, one can be

---

1346 Article8.1 van de Mediawet van 29 december 2008; Hoofdstuk 8 van de Mediawet van 29 December 2008.

1347 *Handleiding Wet Hergebruik Van Overheidsinformatie* (Ministerie van Binnenlandse zaken en Koninkrijksrelaties 2015) <https://open-overheid.nl/wp-content/uploads/2016/01/WEB_88737_handleiding_A5.pdf> accessed 2 February 2020.

penalised under the Dutch Criminal Code. Even though there are cases where the freedom of expression is not fully enjoyed, overall limitations to the Freedom of Expression are only assessed on a case-by-case basis. This is also in line with the fact that there is no concrete legislation on censorship in the Netherlands as well as that the Dutch government gives citizens the right to information which allows for more transparency than the freedom of expression initially confers.

2. Which legislation on the issue of blocking and takedown of Internet content does your country have?

2.1. Introduction

To answer the main question concerning the issue of blocking and takedown of Internet content, the following subjects will be addressed. First and foremost, the legal basis for the blocking and taking down of content on the internet will be discussed. Secondly, the blocking and takedown of content will be looked at in more detail. Lastly, Dutch case law relating to this issue will be analysed.

2.2. Legal basis for the blocking and takedown of Internet content

In the Netherlands, there is no specific regulation on the issues of blocking, filtering and taking down of internet content. However, a wide body of case law exists, which is primarily based on Article 6:196c of the Dutch Civil Code (*Burgerlijk Wetboek*) (DCC). This article lays out the liability exemption for information society service providers (ISPs), which is based on Dutch tort law.[1348] The case law will be dealt with later on in section 2.4. The general right of internet access and its possible restrictions do not have a central place under Dutch law. Measures for blocking and taking down of illegal internet content are scattered over several different forms of regulations, including the Dutch Civil Code (Burgerlijk Wetboek) (DCC), the Dutch Criminal Code (Wetboek van Strafrecht) (DCrC), the Dutch Copyright Act (Auteurswet) and the Dutch Code of Criminal Procedures (Wetboek van Strafvordering) (CCP).[1349]

The Netherlands has one central article on civil liability (Article 6:162 DCC), which states that 'someone who acts wrongfully is obligated to compensate the damages the victim suffered because of his act'. Another important article is Article 240b DCrC, which criminalises the possession, transfer and access of

[1348] The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015; Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' [2008] Master Thesis for the Master Law and Technology, Tilburg University ; B.-J. Koops, 'Cybercrime Legislation in the Netherlands' [2010] Electronic Journal of Comparative Law, vol 14.3.

[1349] ibid.

content related to child-pornography.[1350] Article 26d of the Dutch Copyright Act gives individuals the right to request the court to order intermediaries - whose services are used by third parties to infringe on copyright - to stop providing the related services. Finally, internet content inducing terrorism can be taken down based on Article 126zi DCCP.[1351] In 2012, the Netherlands introduced the principle of internet neutrality (Netneutraliteit) in Article 7.4a(1) of the Telecommunication Act (Telecommunicatiewet).[1352] This article stipulates that only in four extraordinary circumstances is the ISP allowed to take discriminatory measures and, consequently, block the internet content.[1353]

2.3. Blocking of Internet content

The difference between the taking down of and blocking access of content as censoring techniques is quite straightforward. In the case of takedown, the ISP is aware of what content the issue concerns, whereas in the case of blocking, the focus is not on the content, but rather the future.[1354] In addition, when content is taken down, the content as a whole will be removed, while when it is blocked rather than taken down, the illegal internet content stays online, but internet users are denied access.[1355] In Article 54 DCrC, one specific exemption from liability for ISPs has been laid down.[1356] However, its purpose is to provide a general legal basis for making illegal content inaccessible, serving the purposes of seizing criminal offences or preventing new ones to happen.[1357]

2.4. Takedown of Internet content

Notice and takedown (hereafter: NTD) is a concept in which companies or natural persons are requested to make illegal internet content unavailable for the internet users.[1358] NTD as a censoring technique is thus a process used by intermediaries, such as ISPs and online hosts, in response to court orders or allegations that the content is illegal. The content is subsequently removed

1350 Wetboek van Strafrecht; The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015.

1351 Wetboek van Strafvordering.

1352 Telecommunicatiewet; Autoriteit Consument & Markt, 'Netneutraliteit' <https://www.acm.nl/nl/onderwerpen-telecommunicatie-internet/netneutraliteit> accessed 15 February 2020 [Dutch].

1353 ibid.

1354 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015.

1355 M. van der Linden-Smith and A.R. Lodder, Jurisprudentie Internetrecht *2009-2015* (Deventer: Kluwer).

1356 Wetboek van Strafrecht; B.-J. Koops, 'Cybercrime Legislation in the Netherlands' [2010] Electronic Journal of Comparative Law, vol 14.3.

1357 ibid.

1358 Jan-Jaap Oerlemans, 'Filtering the Internet for Law enforcement purposes?' [2013] Leiden Law Blog, Universiteit Leiden. ; Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' [2008] Master Thesis for the Master Law and Technology, Tilburg University.

following the notice. NTD is widely considered in relation to copyright infringement, as well as for cases of libel and other illegal content such as child pornography. As a result, an administrator of the website can be requested to remove the illegal content (Article 240b DCrC). Another example is the takedown of illegal content related to copyright infringements, pursuant to Article 25d Dutch Copyright Act.[1359]

2.5. Case law

The legal framework regarding ISP liability is the result of the implementation of the E-Commerce Directive (Richtlijn *inz*ake elektronische handel).[1360] The Dutch case law that relates to ISP liability, points out different aspects of this type of liability.[1361]

The oldest case relating to the circumstances in which ISPs should act, is one that started in 1996, namely the *Scientology v. XS4ALL* case.[1362] Scientology accused XS4ALL of infringing the copyrights on a text that was written by the founder of Scientology.[1363] Scientology claimed that having a link to unlawful content on the website of XS4ALL is a copyright infringement as it meant that third parties could access it.[1364] The Dutch Supreme Court confirmed the Court of Appeal's decision, which stated that 'in balancing copyright against the freedom of expression, the latter should prevail.'[1365] Moreover, ISPs such as XS4ALL are not publishing the information themselves, but merely providing the means for others to be able to publish.[1366]

Another significant case is *Lycos v. Pessers*. Pessers earned, next to his normal job, 350,000 euros a year by trading in postage stamps on eBay.[1367] A buyer who was not satisfied with his product, designed a website through which he told about how he got 'ripped off' by Pessers.[1368] Pessers subsequently asked Lycos, the

---

1359 Ibid; Wetboek van Strafrecht; Auteurswet; S. Kulk, 'De Aansprakelijkheid van Platforms voor Auteursrechtinbreuken' [2007] Utrecht University [Dutch].

1360 Directive 2000/31/EC of the European Parliament of 8 June 2000 in certain Legal aspects of information society services, in particular electronic commerce in the Internal Market, O.J. 2000, L178.

1361 Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' [2008] Master Thesis for the Master Law and Technology, Tilburg University.

1362 Dutch Supreme Court, Judgement, HR 16 December 2005, NJ 2006, 9.

1363 Ibid; Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' [2008] Master Thesis for the Master Law and Technology, Tilburg University.

1364 ibid.

1365 Dutch Supreme Court, Judgement, HR 16 December 2005, NJ 2006, 9. ; Court of Appeal 's-Gravenhage, 4 September 2003, *NJ* 2003.; The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015.

1366 Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' [2008] Master Thesis for the Master Law and Technology, Tilburg University.

1367 Dutch Supreme Court, Judgement, HR 25 November 2005, NJ 2009, 550.

1368 ibid; Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' [2008] Master Thesis for the Master Law and Technology, Tilburg University.

relevant ISP, to remove the information and to reveal the personal details of the owner of the website. The Dutch Supreme Court ruled that Lycos had to reveal the identity of the person who made the website with the defamatory statements.[1369] As a result, the Court concluded that the Right to Freedom of Expression is not absolute.

The most recent case regarding the topic of ISP liability is IS InterNed Services.[1370] Asylum seeker X was denied a Dutch passport. The Dutch Tax Authority was afraid that X and his partner would leave the Netherlands without paying a tax assessment that they had imposed earlier. The Tax Authority then proceeded to seize money and goods from Asylum seeker X's company called A-Group.[1371] X claimed this move was racist and subsequently made a website, hosted by IS InterNed Services - the ISP in casu - through which he accused the Dutch Tax Authority and the tax inspector of racism. The Court in Haarlem ruled that 'Article 6:196c(4) DCC does not hold an ISP liable if he did not know of unlawful content on their server and removed the illegal information as soon as they are aware of it.'[1372]

In the case Your Hosting, the Court in Overijssel confirmed the ruling in IS InterNed Services, stating that 'a hosting provider such as Your Hostel, is not liable for the content of the websites that are connected to the internet through its server, if the hosting provider i) does not know about the activity or information of an unlawful nature, and, in the case of claim for damages, not reasonably made aware of the activity of information of an unlawful nature, or ii) as soon as he knows that he is reasonably aware of it, promptly erases the information or makes it impossible to access that information (Article 6:196c(4) DDC)'.[1373]

To conclude, the most famous case related to the blocking of internet content is the one of Pirate Bay, where BREIN, a Dutch anti-piracy organisation, received several court orders that forced ISPs to block access to Pirate Bay.[1374] The Court in Amsterdam ordered Pirate Bay to stop copyright infringements and to make its website inaccessible to internet users.[1375]

1369 ibid.
1370 Court of Haarlem, Voorzieningsrechtbank Haarlem 14 May 2008, *LJN* BD1446.
1371 ibid; Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' [2008] Master Thesis for the Master Law and Technology, Tilburg University.
1372 ibid; Burgerlijk Wetboek.
1373 Court of Overijssel, 10 January 2018, *AR* 2018/415.
1374 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015; Court of Amsterdam, 22 October 2009.
1375 ibid.

2.6. Conclusion

It can be concluded that in the Netherlands there is no specific legislation targeting the issue of blocking and taking down of content on the Internet. However, a wide body of case law exists primarily based on Article 6:196c DCC. As mentioned above, a request to block or take down illegal internet content can be based on different articles, which are scattered over different forms of regulations.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

3.1. Difference between civil and criminal law

Unlawful content in civil matters is governed by relevant provisions of the Dutch Civil Code if the wrongful acts lead to civil liability or by provisions of the Copyright Act when it relates to issues on intellectual property rights. For both cases there are multiple articles relating to requests to block, filter, or take down content. However, these issues can also be lodged as part of the Notice-And-Take-Down (NTD) procedure where intermediaries can be ordered to implement effective procedures of this type based on Article 6:196c DCC.[1376] In this context, several Dutch intermediaries have voluntarily adopted a Code of Conduct on NTD,[1377] which sets out the rules on how intermediaries 'are expected to respond to requests for removing content.'[1378] As regarding the enforcement of measures under national law, it is important to mention that in civil law matters any legal person, in which a right is vested, may start proceedings. In contrast, in criminal law matters, only the prosecutor can start a criminal investigation of the unlawful act.[1379]

Illegal criminal content, such as child pornography, is regulated under Article 54a of the Dutch Penal Code (DPC), which authorises the police and the public prosecutor to block or take down content. In addition, the NTD procedure is also deployed in the criminal law context as it is the first option taken by law enforcement authorities before resorting to the procedure in Article 54a DPC. Another significant feature is that general monitoring of internet access is only possible if conducted as part of a criminal investigation. Where it is an issue of

1376 *NSE v. Stichting Brein* NL:GHAMS:2014:3435 [2014] para 3.7.1.

1377 Zenet Mujic, Deniz Yazici, and Mile Stone, 'Freedom of Expression on the Internet' (2012) OSCE, 266.

1378 Joao page Quintais, 'Global Online Privacy Study: Legal Background Report' (2018) University of Amsterdam, Faculty of Law, Institute for Information Law, 134.

1379 ibid. 135.

unlawful content in civil law matters, intermediaries cannot be forced to monitor internet access of users as it is prohibited under Article 15 of the Directive 2000/31 on E-Commerce (the E-Commerce Directive). In both criminal law and civil law matters, non-compliance with the NTD-procedure may lead to the intermediary incurring civil or criminal liability.

3.2. Removing otherwise legal content

Some academics suggest that the Dutch regulatory framework is susceptible to the threat of 'structural over-blocking,'[1380] which is a concept that refers to the unsolicited taking down of otherwise legal information when filtering mechanisms are used. Indeed, filtering is regarded as a 'severe form of censorship'[1381] with implications far more problematic than the actual blocking and taking down of information. This is because filtering mechanisms preclude users or internet service providers (ISPs) from being able to view and assess the real value of the material, resulting in the filtered material being put into an opaque 'filtering bubble' without analysis. Even today Dutch law does not contain the necessary explicit legal basis that would warrant governmental filtering and blocking of internet traffic without the permission of the persons concerned.[1382] Alternatively, ISPs have implemented different filtering mechanisms on a voluntary basis, most notably in the context of catching material pertaining to child pornography.[1383]

3.3. Safeguards

In order to block, take down or filter illegal criminal content the law enforcement authorities rely on the procedure enshrined in Article 54a DPC. Accordingly, an intermediary may be forced to take all reasonable measures to make the contested content inaccessible, but only by means of an order from the public prosecutor. Furthermore, the public prosecutor is able to issue the order only after they have applied for and received a written authorisation from the examining magistrate.[1384] In this case, the written authorisation from the examining magistrate should include a balancing of interests between the

---

1380 Wouter Stol, Henrik Kaspersen, and others, 'Government filtering of websites: The Dutch Case' [2009] 25(3) Computer Law &Security Review 251, 261.

1381 Arno R. Lodder and Kyra Sandvliet, Comparative study on blocking filtering and take-down of illegal internet content – Netherlands (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 494, 496.

1382 Wouter Stol, Henrik Kaspersen, and others, Government filtering of websites: The Dutch Case [2009] 25(3) Computer Law &Security Review 251, 262.

1383 Jacqueline Beauchere, Revenge Porn: Putting Victims Back in Control (Microsoft Blog, 22 July 2015) <https://blogs.microsoft.com/on-the-issues/2015/07/22/revenge-porn-putting-victims-back-in-control/> accessed 3 February 2020.

1384 Criminal Code of the Kingdom of Netherlands (1881, amended 2012) (DPC) Article 54.

Freedom of Expression and the public interest pursued by law enforcement authorities.

The NTD provides an additional condition to the activities undertaken by intermediaries in the online sphere as it requires intermediaries to balance interests when assessing the legitimacy of a lodged complaint. The NTD code of conduct, albeit recognised as a form of self-regulation, introduces transparency to the decision-making process that intermediaries engage in when forced to decide whether a lodged complaint is legitimate and, respectively, whether the contested material should be blocked or taken down. Indeed, where accompanied by effective procedures that allow for a rapid response, the NTD procedure may amount to 'an appropriate tool for balancing the rights and interests of all those involved.'[1385]

3.4. Judicial review

In the Netherlands, Dutch judiciary bodies are responsible for making the decision on blocking, filtering and takedown of illegal internet content.[1386] Indeed, one of the most widely used enforcement measures in the Netherlands is the issuing of a court order that requires an intermediary to block access to an infringing website.[1387] Proceedings typically start before one of the District Courts in the Netherlands. Where a party to the dispute wishes to challenge the action of blocking or taking down of content, they may lodge an appeal with one of the four Courts of Appeal, and later bring the case before the Supreme Court. Important to note is that Article 54a DPC fails to provide guidance as regards the lodging of appeals against criminal law charges as well as that it fails to describe the corresponding conditions and safeguards. The reason for this is that the safeguards and conditions relating to the procedure are based on customary law and the general principle of fair proceedings.[1388]

3.5. Compliance with the case law of the European Court of Human Rights.

When assessing the extent to which national legislation abides by the requirements of the ECtHR case law, it must be reiterated that the Netherlands does not have a specific regulatory framework on the issues of blocking, filtering

---

1385 *Delfi AS v. Estonia* App no 64569/09 (ECtHR, 10 October 2013), para 28.

1386 Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 495.

1387 Joao page Quintais, 'Global Online Privacy Study: Legal Background Report' (2018) University of Amsterdam, Faculty of Law, Institute for Information Law, 136.

1388 Wouter Stol, Henrik Kaspersen, and others, 'Government filtering of websites: The Dutch Case' [2009] 25(3) *Computer Law &Security Review* 257.

and takedown of illegal internet content. Instead, Dutch municipal courts are required to safeguard the balance between the integrity of the online space on the one hand and fundamental human rights on the other hand.[1389] In addition, Dutch judges are precluded from assessing national law in light of the Constitution.[1390] As a consequence, constant reference is made to fundamental rights enshrined in the European Convention of Human Rights and to the EU Charter of Fundamental Rights, as opposed to the Constitution of the Netherlands.[1391] In 2012, the Court of Appeal of Amsterdam outlined a set of characteristics that assist in conducting a balancing exercise between the freedom of speech and other competing interests in the given case.[1392] The characteristics are as follows:

- The nature of the suspicions;
- The severity of the anticipated effects for individuals;
- closely linked to the aforementioned suspicions;
- The severity of the abuse that is communicated;
- The degree to which the statements were rooted in the facts available at the moment of the communication;
- The framing of the suspicions;
- The nature of the medium used for communication;
- The position of the concerned individual.

The ECtHR contends that filtering mechanisms are 'a form of censorship that warrant close attention,'[1393] more so than blocking or taking down content after it has been made available online. Notably, the set of characteristics established by the Dutch court is recognised to be aligned with the spirit and purpose of Article 10(2) ECHR.[1394] To justify an interference under Article 10 ECHR, three cumulative conditions must be fulfilled: the interference must be traced to a legal

1389 The Council of Europe, 'Comparative Study on Blocking, Filtering And Take-Down of Illegal Internet Content' (Lausanne, 2015) 3.

1390 Kingdom of the Netherlands, 'Factsheet on the judiciary in the Netherlands' (*The Netherlands and You*, 21 September 2019) <https://www.netherlandsandyou.nl/latest-news/news/2017/09/21/factsheet-on-the-judiciary-in-the-netherlands> accessed 7 February 2020.

1391 Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 505.

1392 The set of criteria is identified and translated in English by Arno R. Lodder and Kyra Sandvliet, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 494, 504.

1393 Sarah Eskens, Natali Helberger, Judith Moeller, 'Challenged by news personalisation: five perspectives on the right to receive information' [2017] 9(2) Journal of Media Law 259, 282.

1394 Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 504.

basis in national law, it must be necessary in a democratic society and it must be proportionate.[1395]

Nevertheless, some academics argue that there is no legal basis for the implementation of internet filters by, or in behalf of, the Dutch Government[1396] in the servers of intermediaries. Filtering is particularly intrusive because it in a sense creates a 'filtering bubble.'[1397] Article 2 of the Dutch Police Act 1993 warrants specific powers regarding the use of police measures. However, there is no legal basis in Article 2 for Dutch law enforcement authorities to introduce a preventive measure such as filtering as it is in conflict with the fundamental right to freedom of speech as well as the right to privacy.[1398]

3.6. Case law

3.6.1. NSE v Stichting BREIN

Court of Appeal of Amsterdam, ECLI:NL:GHAMS:2014:3435, 19 August 2014

BREIN is a foundation that pursues the objective of combating unlawful exploitation of information carriers.[1399] For the purpose of this case, BREIN initiates litigation procedures for the protection and realisation of its agenda either under its own name or on behalf of its affiliates. NSE - which ceased to exist as a result of the contested judgement - was an operator of a platform for Usenet services. Usenet services were used for discussions as well as for distributing messages that contain images, sound and/or software.[1400] BREIN presented the Court of First Instance with a list of demands, including a declaration that NSE infringed the copyright - and other related rights - of members of BREIN by making reproductions of their work available to third parties via the Usenet services, but without the permission of the right-holder.[1401]

NSE implemented a Notice-and-Take-Down (NTD) procedure, which the Court of Appeal considered to be a commensurate measure with the conditions of Article 6:196c (4)(b) DCC. The NTD allows for expeditious removal of infringing material after its online presence is reported by a user. The Court of Appeal continued in its decision by declaring that the contested judgement could

---

1395 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) Article 10(2).

1396 Wouter Stol, Henrik Kaspersen, and others, 'Government filtering of websites: The Dutch Case' [2009] 25(3) Computer Law &Security Review 255.

1397 Mario Haim, Andreas Graefe, and Hans-Bernd Brosius, 'Burst of the Filter Bubble?' [2017] 6(3) Digital Journalism 330, 333.

1398 Wouter Stol, Henrik Kaspersen, and others, 'Government filtering of websites: The Dutch Case' [2009] 25(3) Computer Law &Security Review 256.

1399 NSE v. Stichting Brein (n 1) para 3.1.

1400 ibid. para 3.1.4.

1401 ibid. para 3.2.

not be upheld for the reason that it imposed the requirement to filter all incoming binaries for unauthorised content.

In the case at hand, the injunction issued on NSE effectively amounts to a general monitoring obligation, which exceeds the limitations of the power to impose a prohibition or order arising from Article 15 of the E-Commerce Directive.[1402]

The judgment issued by the Amsterdam Court of Appeal confirms that the procedure of Notice-and-Take-Down is an appropriate measure consistent with the requirements of Article 6:196c (4)(b) DCC, despite the fact that there is no Dutch statutory basis for the NTD procedure. Moreover, the effectiveness of such a procedure can be measured by the extent to which - and the speed with which – infringing material is removed.[1403]

3.6.2. Case C-610/15 Stichting Brein EU:C:2017:456

Ziggo and XS4ALL are internet access providers, which allow their users to access the online sharing platform called Pirate Bay. The platform is used for sharing content. However, most of the content on Pirate Bay is protected by copyright, but without the consent of the right-holders. BREIN is a Dutch foundation that represents the interests of copyright right-holders. BREIN lodged a claim with the Dutch Court for an order that would require Ziggo and XS4ALL to block the domain names and IP addresses of Pirate Bay. The Supreme Court of the Netherlands halted the proceedings to lodge a request for preliminary ruling with the European Court of Justice, seeking to ascertain whether Pirate Bay is 'communicating to the public' and thus infringing copyright.

The CJEU found that the activities performed by Pirate Bay – namely, the making available of content on the internet, even though the content is typically copyrighted – amounts to 'communication to the public' within the meaning of Article 3(1) Directive 2001/29/EC. As a result, the CJEU is authorised to request that blocking measures are taken against Pirate Bay. This effectively directed the case back to the Dutch Supreme Court for the final decision.

Interesting to note is that the CJEU did not extensively consider the balancing exercise between the competing interests of the copyright right-holders and those that use the internet services. However, the Advocate-General at the Supreme Court in the Netherlands did balance the interest of the copyright

[1402] ibid. para 3.6.6.

[1403] Gerechtshof Amsterdam 19 augustus 2014 (NSE), ECLI:NL:GHAMS:2014:3435 (*Internetrechtspraak,* 16 February 2020) <https://internetrechtspraak.com/gerechtshof-amsterdam-19-augustus-2014-nse-eclinlghams20143435/> accessed 16 February 2020.

infringement against the freedom of information of the ECHR,[1404] after which it was sent back to the Amsterdam Court of Appeals for further consideration.[1405] The fact that the Dutch Supreme Court did do the balancing exercise is significant, because it resulted in the decision that Pirate Bay need not be blocked. In fact, it gave internet service providers time to prove that 'having access providers block internet addresses is neither an effective nor a proportionate measure to deal with online copyright infringement.'[1406]

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In the Netherlands, self-regulation with regards to the blocking and taking down of internet content does exist in the form of the Notice-and-Take-Down Code of Conduct (NL), which from here on out will be referred to as the Code. This Code was put into place in 2008 by the Dutch government, individual businesses and interest groups. It can be considered to be self-regulation in the sense that it does not establish any statutory obligations, but rather helps parties to comply with the existing legal framework in the form of providing them with descriptions of procedures as to the removal of information on the internet on the request of third parties. In addition, it describes how the online sector handles complaints about illegal content on the internet. However, the Code does not prohibit one from taking an issue with regards to the removal of content before the courts, in the case of an issue regarding civil law, or to make an official report to the police, in the case of an issue regarding criminal law, even if the content in question has already been taken down.

The Code consists of 7 Articles. Article 1 describes the scope of the Code: to establish a procedure to deal with reports of unlawful content on the internet. Important to note is that the code is not applicable to situations in which other statutory obligations or liabilities are applicable for intermediaries on the basis of legislation and jurisprudence (Article 1c). In principle this establishes that civil and criminal law issues take precedence over the Code. Article 2 establishes several important definitions, such as those relating to the definition of a report,

---

1404 Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 505.

1405 Supreme Court of the Netherlands ECLI: NL: HR: 2018: 1046 <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:PHR:2018:202> last accessed 16 February 2020.

1406 TBO, 'Dutch Supreme Court remands Pirate Bay Case for Review' (Trademarks and Brands Online, 4 July 2018) <https://www.trademarksandbrandsonline.com/news/dutch-supreme-court-remands-pirate-bay-case-for-review-5265> accessed 16 February 2020.

the notifier, the content provider, the organisations, the intermediary, and the actual inspection. To begin with the report: 'a report concerns the reporting by a notifier of alleged unlawful content on the internet to an intermediary, with the objective of having this content removed from the internet',[1407] which means that the report is the information passed from the claimant to the intermediary. The notifier can be anyone given that the definition in the Code is that they are a person or an organisation that makes the report.[1408] The content provider is defined as the person or organisation that has placed the content on the internet,[1409] the intermediary as the provider of the service on the internet (Article 2d) and the inspection as a legally appointed governmental service that has the competent powers to investigate (Article 2e). In addition, the Code states that to ensure effectiveness, it is preferable to make a report only when it is likely that the notifier and the content provider will be unable to reach an agreement on their own.[1410] There is, however, no obligation to actually try to reach such an agreement.

The reports can be delivered in two different forms. The first is in regard to criminal offences, in which case the intermediary must verify that the report originates from an inspection or investigation service and otherwise from the Public Prosecutor's office.[1411] The second is deemed by the Code as 'other than those stated in Article 4a'.[1412] This can be understood to mean that these are in regard to issues of civil law. A report like this should consist of important information regarding the alleged unlawful content, including a description as to why the content is unlawful and why the intermediary is being approached as the most appropriate party to deal with the matter. This is further dealt with in Article 5, which establishes that the party to deal with the report is defined as the intermediary.[1413] Article 3 highlights the fact that intermediaries have their own Notice-and-Take-Down procedures that are consistent with the Code and that they must be accessible to the public.[1414]

Article 6 describes the possible actions to be taken by the intermediary. In the event that the content is deemed unequivocally unlawful, the intermediary ensures that the content is immediately removed.[1415] In the event that the content

[1407] Notice-and-Take-Down Code of Conduct (NL), Article 2a.
[1408] Notice-and-Take-Down Code of Conduct (NL), Article 2b.
[1409] Notice-and-Take-Down Code of Conduct (NL), Article 2c.
[1410] Notice-and-Take-Down Code of Conduct (NL), Article 4.
[1411] Notice-and-Take-Down Code of Conduct (NL), Article 4a.
[1412] Notice-and-Take-Down Code of Conduct (NL), Article 4b.
[1413] Notice-and-Take-Down Code of Conduct (NL), Article 5.
[1414] Notice-and-Take-Down Code of Conduct (NL), Article 3.
[1415] Notice-and-Take-Down Code of Conduct (NL), Article 6b.

is not unequivocally unlawful, the intermediary informs the notifier of this.[1416] However, when it relates to a case of content that is not unequivocally unlawful, Freedom of Expression can be at stake given that when lawful content is removed, Freedom of Expression is restricted as a result. In addition, one has to consider that an intermediary is not equipped to deal with the evaluation of reports as the abovementioned. This could lead to mistakes such as the incorrect decisions to remove content or to not remove it where it should be removed. In the case of an intermediary not being able to come to a decision, the intermediary must inform the content provider about the report with the request to either remove the content or contact the notifier.[1417] This mechanism helps to protect freedom of expression, because content that might be unlawful is not removed immediately, but rather addressed and considered again. Furthermore, the intermediary should exercise due caution in the execution of the measures that have to be taken in order to ensure that the removal of any content that is not referred to in the report is avoided.[1418] This also helps to protect Freedom of Expression as it prescribes that any content that is not deemed unlawful, should not be removed. However, the issue that arises in cases similar to those in Article 6a arise here as well: it is not always clear exactly to which extent the content is unlawful.

Not only is there an issue with Freedom of Expression when it comes to situations that fall under Article 6c. In fact, in some cases the content provider can be unwilling to make him or herself known to the notifier. In those cases, the intermediary can decide to provide the notifier with the content provider's name and contact details, or to remove the content.[1419] In the cases where the intermediary decides to remove content, the Freedom of Expression could be infringed. It could be the case that following a report the intermediary decides to wrongfully remove lawful content because the content provider refuses to make him or herself known to the notifier. However, prior to the removal, the content provider must have a chance to defend themselves. The problems regarding Freedom of Expression that could arise as a result of the Code could be countered by means of a grievance redressal mechanism. Such a mechanism could be considered useful in the case of a wrongful takedown. However, the Code does not provide for such a mechanism.

To conclude, the issue of blocking and taking down internet content is largely self-regulated by the private sector. The main source for organisations in the

[1416] Notice-and-Take-Down Code of Conduct (NL), Article 6a.
[1417] Notice-and-Take-Down Code of Conduct (NL), Article 6c.
[1418] Notice-and-Take-Down Code of Conduct (NL), Article 6d.
[1419] Notice-and-Take-Down Code of Conduct (NL), Article 6c.

Netherlands is the Notice-and-Take-Down Code of Conduct. The Code provides individuals and organisations with clear rules and guidelines as to when content should be removed from the internet, as well as to when it should not. However, there are no explicit safeguards within the Code to ensure the freedom of expression. There are mechanisms in place in other sources which help to prevent lawful content from being removed which can be consulted on a case-by-case basis. Given that the Code is not a binding measure but rather a guideline for individuals and organisations, modes of relief are not the primary concern.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

This section will investigate whether the Netherlands applies specific legislation on 'the right to be forgotten' or in other words the 'right to erasure'. European Union law is applicable in the Netherlands and has a great influence over national legislation on privacy and data protection. In addition, the Netherlands also guarantees the constitutional right to privacy under Article 10 of the Dutch Constitution. One of the primary guarantees of protection of personal data on the level of the European Union can be found in Article 12(b) of Directive 95/46/EC which allows individuals to request erasure of their personal data in order to protect themselves against unwanted publication of personal facts.[1420]

In 2014, in the case of Google Spain,[1421] the main issue of the proceedings concerned the 'Right to be Forgotten' (RTBF). As a result, a landmark ruling for the European Union was given which established that individuals can request the delisting of information from search results. Search engines such as Google, Bing or Yahoo must delist URLs from across the Internet that are inaccurate, inadequate or no longer relevant - or where they contain information that is excessive in relation to their purposes and in the light of the time that has elapsed.[1422] Therefore, a data subject has a right to request a given commercial search company to remove links to their private information. However, this right is not absolute nor automatic given that the judgement in Google Spain requires that search engine operators make the assessment of whether an individual's right to privacy outweighs the public's right to access information.[1423] In addition, the court established the requirement that the information must not be

[1420] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.
[1421] Case C-131/12 Google Spain and Google EU:C:2014: 317, [2014] ECR.
[1422] ibid, para 92.
[1423] ibid, para 91.

relevant anymore. The right to request the removal of links only arises where the controller no longer needs the data for the purposes for which they were lawfully collected or processed, where withdrawal consent has been given or where an objection right was exercised successfully.

Even though this case only took place in 2014, there was already data protection prior to the ruling in Google Spain. In the Netherlands, the right to informational privacy was first codified by the Act on the Registration of Personal Data (*Wet Persoonsregistraties*) of 1988.[1424] Later, this act was replaced by the Act on the Protection of Personal Data (*Wet bescherming persoonsgegevens*) (WBP) as a result of the transposition of the Directive 95/46/EC. Under the new act the concept of the Right to be Forgotten was called 'the Right to Erasure' and it was protected under Article 36 of Dutch Data Protection Act.

When the new legislation on privacy and data protection came into existence in the European Union, the WBP was replaced by the Dutch Implementation Act (*Uitvoeringswet AVG*). The Implementing Act regulates the protection of personal data and implements the General Data Protection Regulation (GDPR)[1425] in the national system.[1426] In addition, it follows a policy- neutral approach, meaning that the WBP was maintained where possible under the GDPR.[1427]

The Google Spain ruling was incorporated into Article 17(2) of GDPR. As a result, the principle of the 'right to be forgotten' was codified into European legislation. As mentioned above, this Regulation was implemented into the Dutch national system and therefore Article 17(2) of the GDPR - more specifically the 'right to be forgotten' - is applicable in the Netherlands by reason of direct effect. Article 17(2) states that the data subject has the right to request the erasure of personal data concerning them without undue delay from the controller and that the controller has the obligation to erase personal data without undue delay. The article also outlines specific circumstances under which the Right to be Forgotten is applicable.

Even though there is legislation on the Right to be Forgotten, when it comes to analysing the application of the Right to be Forgotten, one should focus on the

---

1424 A.J. Verheij (2016) The right to be forgotten – a Dutch perspective, International Review of Law, Computers & Technology, 30:1-2, 32-41, DOI: 10.1080/13600869.2015.1125156.

1425 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1426 *Autoriteit Persoonsgegevens* (Dutch Data Protection Authority website) <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/algemene-informatie-avg> accessed on 25 February 2020.

1427 Data Protection Laws of the World: the Netherlands, 2017 DLA Piper, page 2.

judgment of the landmark case *Google Spain* as it sets out a general understanding of the right to be forgotten that must be applied in all European Union Member States. However, it is important to mention how the Dutch courts interpreted the right to erasure before 2014.

A few Dutch cases are worth mentioning when taking a look at the right to erasure in the Netherlands prior to the Google Spain judgment. The facts of the first case were as follows: In 1944, Mr. van Gasteren had been criminally convicted for a murder. After the end of the Second World War, Mr. van Gasteren requested and obtained a pardon by arguing that the victim presented a threat to the resistance movement.[1428] In 1990, the national newspaper Parool published three articles arguing that the death of the victim was not an act of resistance but rather a brutal murder. Van Gasteren decided to sue Parool for damages on the basis of defamation. In the judgement the Supreme Court established that one has the right to be left alone.[1429] In addition, the general right to personality encompasses the right not to be confronted with a conviction that dates back more than 40 years ago.[1430] The Supreme Court also stated that in order to publish anything related to a crime years after conviction there would have to be special reasons of public interest that would justify this in addition to the fact that it must be based on accurate research.

Another example concerns an individual who had been convicted in 1995 for the sexual abuse of minors who had been entrusted into his care.[1431] In 2009, a Dutch website published his name and address in order to alarm the parents living in the neighbourhood. Consequently, flyers with his personal data were distributed around the neighbourhood and he and his family had to move. The plaintiff sued the website and requested that further publications would be forbidden. The Court of Utrecht agreed to this request, stating that the publications of his personal data could have foreseeable serious personal consequences for the plaintiff and his family. In other words, publications like these would stimulate people 'to take the law into their own hands'.[1432] In principle, there is a right to not be confronted with one's past after a certain time has elapsed as mentioned in the case with Mr. van Gasteren.[1433] However, it is not clear when this right comes into existence, although from the mentioned

1428 A.J. Verheij (2016) The right to be forgotten – a Dutch perspective, International Review of Law, Computers & Technology, 30:1-2, 32-41, DOI: 10.1080/13600869.2015.1125156, page 36.
1429 HR 6 Januari 1995, ECLI:NL:HR:1995:ZC1602 (Parool/Van Gasteren).
1430 ibid.
1431 Rb. Utrecht 15 December 2010, ECLI:NL:RBUTR:2010:BO7295.
1432 A.J. Verheij (2016) The right to be forgotten – a Dutch perspective, International Review of Law, Computers, page 37.
1433 A.J. Verheij (2016) The right to be forgotten – a Dutch perspective, International Review of Law, Computers & Technology, 30:1-2, 32-41, DOI: 10.1080/13600869.2015.1125156, page 39.

case law it can be said that it very much depends upon the individual circumstances of the case. As a result of this case, multiple principles relating to the right to be forgotten were either established or elaborated upon. Eventually the right to be forgotten developed over time through case law.[1434]

After having taken a look at the application of the right to be forgotten prior to 2014, one can take a look at the way the national courts applied the ruling established in Google Spain and compare it to how it differs. The first case in the Netherlands that related to the right to be forgotten after the judgement in Google Spain was about a convicted criminal and the facts were as follows: in 2012, a Dutch TV channel aired a programme that features hidden camera footage of a man discussing with an assassin what the best way is to kill a competitor. The programme referred only to his first name and the initial of his last name: Arthur van M. This footage was used as evidence in a criminal case against him and he was convicted and sentenced to six years imprisonment for attempting to incite an assassination. As a result, if one were to look for Arthur van M on the internet a set of URLs would appear relating to this crime. Arthur van M wanted some of these URLs to be delisted. In addition, there were pages that already displayed a message that 'some results may have been removed under data protection law in Europe'. He submitted five claims to the District Court of Amsterdam, requesting that Google should delist certain search results.[1435] In the appeal, the Court emphasised that the criminal had been convicted in the first instance[1436] and that the publications with his name are results of the convictions and are therefore of public interest. Another argument was given: the publications do not refer to his full name. Therefore, the Court of Appeal rejected all five of his claims. Here, the Court followed the same reasoning as in the cases before the Google Spain ruling and the GDPR.

However, there is an example of another case where the Court ruled differently. This case involves a contractual relationship between a partner at KPMG - a company that provides audit, tax and advisory services - and a contractor that had to build a new house for this individual. Their dispute related to late payments and this was published by the largest Dutch newspaper, De Telegraaf. The article reports that the partner of a large company is unable to move into his new house due to the fact that the contractor changed the locks as the partner had not paid a bill. When the partner requested the removal of the article, Google refused and stated that the information on the website was relevant for public interest and that it was not considered out-dated. The District Court of

[1434] ibid.
[1435] Rechtbank Amsterdam, 18 September 2014, ECLI:NL:RBAMS:201 4:6118.
[1436] Gerechtshof Amsterdam, 31 March 2015, ECLI:NL:GHAMS:2015 :1123.

Amsterdam emphasised that search engines play an important role in society, and that if they were[1437] subject to too many restrictions, their function would be compromised. As in other cases, the Court put two rights at stake: the right to privacy on the one hand, and the Freedom of Expression and freedom of information on the other hand. It is stated that the KPMG partner requested to move the search results relating to the unpaid bill to the bottom of the search results. Google argued that this was not possible and therefore the Court rejected the partner's claim. In this case the court focused on the lawfulness of the search results rather than the lawfulness of the publication. If the substance of the publication is the issue, the individual should address the publisher and not the search engine operator.[1438] However, it is noticeable that the Dutch Courts tend to prioritise the Freedom of Expression.[1439]

It can therefore be concluded that the Netherlands does not have its own specific legislation on the Right to be Forgotten, but rather applies European legislation and case law. However, in certain cases the national courts might take a different perspective and basis of reasoning when it comes to the right to be forgotten. However, this does not mean that the outcome of the cases would necessarily be different than if they were brought before the European courts.

6. How does your country regulate the liability of internet intermediaries?

The liability of intermediaries for not tackling any circulating criminal content is regulated by Article 54a DCC. If the intermediary has 'taken all measures which can be reasonably expected from it'[1440] upon receipt of the order of the public prosecutor, they shall not be prosecuted. An intermediary may also incur civil liability, as pursuant to Article 6:196c DCC, which is a national transposition of the E-commerce Directive. Under this provision, three types of internet service providers - mere conduit providers, catching providers and hosting providers - are able to escape liability by fulfilling the relevant prescribed requirements.

1437 Rechtbank Amsterdam, 13 February 2015, ECLI:NL:RBAMS:2015:716.

1438 See more in-depth analysis: Stefan Kulk and Frederik Zuiderveen Borgesiu, Freedom of Expression and 'Right to Be Forgotten' Cases in the Netherlands After Google Spain, EDPL Freedom of Expression and 'Right to Be Forgotten', volume 1, issue 2, pages 113-124.

1439 ibid.

1440 Bert-Jaap Koops and Marga Groothuis, 'Constitutional Rights and Technology in the Netherlands' in Ronald Leendes, Bert-Jaap Goops, and Paul De Her (eds.) *Constitutional Rights and New Technologies* (Asser Press, 2008), 183.

6.1 Does an obligation to implement the measures for blocking and taking down content exist?

Intermediaries can in principle be subject to the obligation of blocking or taking down unlawful content by means of a Court order. In criminal law matters, an intermediary presented with the order of a prosecutor, where the latter has received prior written authorisation from the examining magistrate, is under the obligation to undertake all reasonable measures to make the content inaccessible.[1441] However, if the prosecutor's order is not corroborated by a written authorisation from the magistrate, the intermediary will not incur criminal liability by disobeying an investigative officer's requests for blocking or taking down illegal content.[1442] Furthermore, once the intermediary has complied with the order, it no longer has the right to challenge it in a court of law.[1443] A similar obligation exists in civil law cases where a court order or an injunction may be issued for the termination or prevention of an infringement, which can either be blocking or removing the content. Such an obligation is enshrined in Article 6:196c(5) DCC.

Intermediaries are also subject to the obligation to abide by the NTD procedure, despite the fact that it is a voluntarily construed code of conduct by businesses and interest groups alike. Thus, an intermediary will incur liability if the required measures for making the content inaccessible were not taken when it was otherwise necessary; in other words, when the intermediary came to the wrong conclusion during the process of balancing the competing interests they will still be prosecuted. Therefore, if an intermediary, upon receiving the notification and after becoming aware of the illegal material circulating, fails to block the content or take it down, they will incur criminal or civil liability.

6.2 Are there any safeguards in place for ensuring the protection of freedom of expression online?

The phrasing of Article 7 of the Dutch Constitution is considered to be relatively strict in granting adequate protection of Freedom of Expression in a digital

---

1441 Article 54 DPC.

1442 Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 497.

1443 Secretary-General of the European Commission, 'Commission Staff Working Document Impact Assessment: Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online' (2018) SWD(2018)409 final, 131 <https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkrs7l664lz7> accessed 13 February 2020.

environment.[1444] Article 7 includes the press, broadcasts on radio and television and other means of expression. However, it is still unclear whether Article 7 protects the expression of ideas online, which leads to legal uncertainty.

While some academics engage in technical debates and analysis over the phrasing of the provision, the Dutch judiciary has already openly granted protection to the Freedom of Expression online by means of a conjoined application of Article 7 of the Dutch Constitution and Article 10 ECHR. Notably, the courts do not specify which of the paragraphs of freedom of expression rely on,[1445] choosing instead for an overarching interpretation of its purpose. Thus, the freedom of expression in the digital space is safeguarded by the Dutch judiciary through application of Dutch and European law.

Overall, the Netherlands is regarded as one of the leading nations in the protection of Freedom of Expression in the digital space. In 2011, the Netherlands set the foundations for an international coalition of 'countries who stand up for Freedom of Expression on the Internet.'[1446] During the years, the coalition has grown from 18 members to 31, where all governments involved are dedicated towards advancing the Freedom of Expression on the internet in a coordinated manner.[1447]

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1. General remarks on the subject matter

The issue presently researched concerns one of the most progressive fields of law and, by its very nature, is inherently connected to technological developments. Therefore, one can make the credible assumption that law and regulations on internet censorship in the Netherlands will evolve alongside technological advancement. Through both interpretation and new laws, it is

[1444] Bert-Jaap Koops and Marga Groothuis, 'Constitutional Rights and Technology in the Netherlands' in Ronald Leendes, Bert-Jaap Goops, and Paul De Her (eds.) Constitutional Rights and New Technologies (Asser Press, 2008), 181.

[1445] Bert-Jaap Koops and Marga Groothuis, 'Constitutional Rights and Technology in the Netherlands' in Ronald Leendes, Bert-Jaap Koops, and Paul De Her (eds.) Constitutional Rights and New Technologies (Asser Press, 2008), 182.

[1446] Wolfgang Benedek and Matthias C. Kettemann, 'Freedom of Expression and the Internet' (2013) Council of Europe Publishing, 160.

[1447] The Freedom Online Coalition <https://freedomonlinecoalition.com/about-us/history/> accessed 15 February 2020.

possible to assume that, within five years, fields of online censorship will look somewhat different to what they look today. It has already been highlighted in earlier sections of this report that Dutch courts, together with academics, are interested in moving censorship from the legal field to the online world. Nonetheless, it remains unclear how the legislator will react to these new societal trends.

The following chapter will present analysis of current changes and developments in online blocking and takedown activities, liability of internet intermediaries (hereafter referred to as: ISP liability) and the right to be forgotten (also known as the right to erasure) in the Netherlands. It will seek to deliver a critical outline of possible developments in these fields of internet censorship. Moreover, this chapter will examine existing Dutch legislation and aim to best predict further legislative action that could strengthen rules on internet censorship in the Netherlands.

7.2. Internet censorship: more than just a national regulatory issue

7.2.1. Blocking and taking down online content

It is notable that the various form(s) of internet censorship adopted in various countries are shaped by respective national political ideologies.[1448] The Netherlands, known for its freedom of press and freedom of expression, tends to adopt a similar attitude of freedom to the question of internet censorship.[1449] Therefore, one could argue that Dutch legislation regards online freedom of expression with equal importance to freedom of expression in the offline world; when limiting content on the Internet, The Netherlands will ensure that it refrains from enacting laws that make online censorship stricter. Accordingly, only when online content creates danger for public safety, national security or core democratic and constitutional values, will the Dutch government interfere. An example of this lies in the fact that a legal provision which blocks internet content is specifically stated in the Dutch Criminal Code in relation to danger to the public.[1450] It is invoked for offences of a criminal nature only, such as would be the case in regard to the viewing of child pornography. To further exemplify

[1448] Justin Clark et al, 'The Shifting Landscape of Global Internet Censorship.' (2017) Berkman Klein Center for Internet & Society Research Publication 3.

[1449] Alexandra Gowling, 'The Netherlands ranks first globally for press freedom' (*I am Expat* 8 March 2014) <https://www.iamexpat.nl/expat-info/dutch-expat-news/netherlands-ranks-first-globally-press-freedom> accessed 5 February 2020.

[1450] Criminal Code of the Kingdom of the Netherlands (1881, amended 2012) art 54a.

this fact, no legislation on internet censorship can be found in Dutch administrative or civil codes.[1451]

Nonetheless, the above-mentioned facts do not dismiss any future struggles the Dutch government may face in this field of IT law. The main factor which may challenge effectiveness of Dutch censorship laws is movement of prohibited content under Dutch law to bigger, international platforms outside of Dutch jurisdiction.[1452] Such movement may require new Dutch court rulings on the question of extra-territorial jurisdiction and this possibly providing for further development of Dutch internet censorship laws on online content control. In this regard, theories of international private law may play a crucial role. Consequently, one may argue that the Netherlands prefers its national courts to develop pragmatic solutions to internet censorship issues on a case-by-case basis, as opposed to the direct application of written legislation.[1453]

The involvement of the Court of Justice of the European Union (hereafter referred to as: the CJEU), in this matter, should not be undermined either. It should be stressed that European Union (hereafter referred to as EU) law contains various legal provisions which are connected to the matter of internet content control. Even though EU case law has not yet concerned the Dutch legal system directly, the CJEU has already delivered judgements on extraterritorial jurisdiction of the Internet. Bearing in mind that the CJEU's interpretation of EU law is binding on all Member States, it can be concluded that: with new rulings, new concepts and practices are established. This is proven by the fact that in many other EU Member States, such as France and Italy, the matter of taking down and blocking online content is more prominent than in the Netherlands.[1454] Consequently, future preliminary referencing procedures – by said states – to the CJEU may result in new interpretation of EU law on the matter of internet censorship.

Lastly, the possibility of higher governmental involvement can be considered. Without having the ability to take down and block internet content (unless the offence is criminal in nature–as previously emphasised), various State actors can

---

1451 Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 495.

1452 Justin Clark et al, 'The Shifting Landscape of Global Internet Censorship.' (2017) Berkman Klein Center for Internet & Society Research Publication 4.

1453 The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015, 13.

1454 phys.org, 'France and Netherlands plan Internet anti-censorship drive' (*phys.org* 25 May 2010) <https://phys.org/news/2010-05-france-netherlands-internet-anti-censorship.html> accessed 7 February 2020.

join online public spaces and engage in discussions.[1455] Such engagement allows these said actors to indirectly control activities on the internet and to prevent illegal activities from occurring. In conjunction to this method, one can also consider the role of soft rules, and their applicability to internet censorship. For example, it is notable that the Dutch government tends to agree with internet platforms, allowing for the latter to control the content published on their respective domains by their own private means.

7.2.2. ISP Liability

ISP liability in the Netherlands is now primarily governed by the E-commerce Directive.[1456] The application of this Directive differs from state to state. Through a minimum harmonisation process, it allows for the Netherlands to adopt stricter rules on ISP liability; if the Dutch government would consider such stricter rules appropriate. Nonetheless, several important issues remain undiscussed within this legal document. In particular, the Directive fails to cover the matter of the protection of information that the location tool providers. Thus, it will be the Netherlands' responsibility to further develop this area of ISP liability law. Accordingly, this development will rely on the will of the legislator to provide the ISPs with more certainty and forgeability of legal actions which can be taken against them.[1457]

Additionally, similar to the previous section of this chapter, ISPs will continue playing a big role in private censorship procedures. Thus, they will be in charge of balancing public interests and human rights while simultaneously deciding on the elimination of inappropriate content from the Internet.

7.2.3. Right to be Forgotten

The right to be forgotten, firstly examined by the CJEU in its case law,[1458] now plays an important role in Dutch legislation. The Dutch courts' reasoning on this matter usually mirrors the reasoning presented by the CJEU. Accordingly, right to erasure is seen as an imperative right provided by EU law and prevails over other interests, such as commercial interest or a right to receive information. Dutch courts extensively try to balance private and public interests while also

[1455] Justin Clark et al, 'The Shifting Landscape of Global Internet Censorship.' (2017) Berkman Klein Center for Internet & Society Research Publication 22.

[1456] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178.

[1457] Soma J and Norman N, 'International Take-Down Policy: A Proposal for WTO and WIPO to Establish International Copyright Procedural Guidelines for Internet Service Providers', (2000) 22(391) Hastings Communications and Entertainment Law Journal 13.

[1458] Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014] ECLI:EU:C:2014:317 para 63.

considering the Right to be Forgotten. A successful incorporation of this right can be seen through the fact that around 17.000 requests for erasure come from Dutch citizens to Google. Therefore, it can be assumed that there will not be many major changes within this legal matter, unless the CJEU itself delivers a new interpretation of the General Data Protection Regulation[1459] (hereafter, referred to as: the GDPR). The Right to be Forgotten is already well-established[1460] and thus, the only features which may appear in the foreseeable future can be connected to the strengthening of data protection observance in the Netherlands.

Nonetheless, it should be reiterated that Dutch courts are constantly seeking to engage in a deeper balance of public and private interests when it comes to the right for erasure, more-so than is currently done by the CJEU. This is accordingly illustrated in Dutch national case law. However, this also depends on the nature of the channel through which the information was made available to the public.[1461]

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

In the Netherlands both the Right to a Freedom of Expression and the prohibition of hate speech can be found in the national legislation, as well as in the international treaties to which the Netherlands is party. The Netherlands has, however, not yet issued explicit legislation concerning the Internet and blocking, filtering and taking down of illegal internet content. This does not, however, mean that current legislation concerning freedom of speech and prohibition of hate speech is not applicable to online situations. Non-legislative approaches have been implemented to combat specific types of hate speech online. Furthermore, as a member of the European Union (hereafter referred to as: the EU), the Netherlands is subject to European law and the case law of the Court of Justice (hereafter referred to as: the CJEU), including the CJEU ruling on interpretation and application of EU law. The Netherlands follows the monistic

[1459] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119 art 17.

[1460] Jeffrey Rosen, 'The Right to Be Forgotten' (2012) 64(88) Stanford Law Review Online 88-92, 89.

[1461] Céline van Waesberge, 'Dutch surgeon successfully invokes the right to be forgotten' (Loyens&Loef 4 March 2019).

doctrine which means international treaties and norms are part of its legislation, without having been transposed by national law.[1462] Thus, the European Convention on Human Rights (hereafter referred to as: the ECHR) can also be invoked in Dutch Courts. These Courts will then have to consider rulings made by European Court of Human Rights (hereafter referred to as: the ECtHR) when applying the ECHR.

8.1. Freedom of expression

Freedom of Expression in the Netherlands is protected by Article 7 of the Dutch Constitution (Grondwet), Article 10 of the ECHR, Article 11 of the Charter of the Fundamental Rights of the European Union (hereafter referred to as: the CFR) and Article 19 of the International Covenant on Civil and Political Rights (hereafter referred to as the ICCPR).[1463] Freedom of expression in the Dutch Constitution is categorised into: freedom of the press, freedom of the media and Freedom of Expression by other means.[1464] According to the ECHR, freedom of expression includes: 'the freedom to hold opinions and the freedom to receive and impart information and ideas'. According to both the ECtHR case law and commentary on the Constitution, the protection of the freedom of expression is not limited to expressions, ideas, feelings or information that are favourably received and that are considered innocent or neutral.[1465] This does not mean that the right to Freedom of Expression is an absolute right. Limitations on the Freedom of Expression, within the Dutch Constitution, can only be enacted by an act of parliament.[1466] Freedom of expression in the ECHR must be either limited by a prescribed law, be necessary in a democratic society or be for one of the legitimate aims listed in Article 10(2) ECHR. Moreover, Article 17 ECHR – which prohibits the abuse of rights – precludes protection by the Convention where the comments made amount to hate speech and negate the fundamental values of the Convention.

1462 Grondwet voor het Koninkrijk der Nederlanden 2002 , 24 August 1815, Staatsblad van het Koninkrijk der Nederlanden [Stb.], art 93.

1463 Grondwet (n 1) art 7; European Convention on Human Rights (ECHR) art 10; Charter of the Fundamental Rights of the European Union [2007] OJ C 303/17, art 11; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 19.

1464 Grondwet voor het Koninkrijk der Nederlanden 2002 , 24 August 1815, Staatsblad van het Koninkrijk der Nederlanden [Stb.], art 93.

1465 D.E. Bunschoten, 'Artikel 7' in J.H. Nieuwenhuis, C.J.J.M. Stolker, mr. W.L. Valk (eds) *Grondwet en Statuut Tekst & Commentaar* (5th ed, Wolters Kluwer 2018); *Handyside v. the United Kingdom*, App No.5493/72, (ECtHR, 7 Decemeber 1976), para. 49, <http://hudoc.echr.coe.int/eng?i=001-57499>.

1466 The right is subjected 'to everyone's responsibility under the law.'

8.2. Freedom of Expression Online

The human rights and fundamental freedoms stated in the ECHR apply both offline and online.[1467] Accordingly, the ECtHR has stated that 'the Internet has become one of the principal means for individuals to exercise their right to Freedom of Expression today: it offers essential tools for participation in activities and debates relating to questions of politics or public interest.'[1468] Furthermore, paragraph three of the Dutch Constitution – which covers the Freedom of Expression through means other than printing press and broadcasting – includes expressions or communications via the Internet. Therefore, it can be concluded that Freedom of Expression online is protected by the same general provisions as offline, and so will also be subjected to the same limitations.

8.3. Hate speech

Hate speech is one of the limitations to the Freedom of Expression. There is no universally accepted definition of hate speech. Most definitions include some form of the words 'incite hatred.' Some definitions are broader and include hate speech that target groups and/or incite violence. In Recommendation No. R (97) 20 of the Committee of Ministers of the Council of Europe, hate speech was 'understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin'. In EU law, hate speech is defined as the 'public incitement to violence or hatred directed to groups or individuals on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin.'[1469] The Dutch Criminal Code prohibits both insulting a group and incitement to hatred.

The Dutch Criminal Code penalises insulting a group under Article 137c: Anyone who publicly, orally, in writing or graphically, intentionally expresses himself insultingly regarding a group of people because of their race, their religion or their life philosophy, their heterosexual or homosexual orientation or their physical, psychological or mental disability, shall be punished by

[1467] Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users, 16 April 2014 <https://rm.coe.int/16804d5b3>.

[1468] *Ahmet Yildirim v. Turkey* App no 3111/10 (ECtHR, 18 December 2012), para 54, <http://hudoc.echr.coe.int/eng?i=001-115705>.

[1469] Summary of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law, 15 June 2014 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:l33178>.

imprisonment of no more than a year or a monetary penalty of the third category.

The Dutch Criminal Code penalises incitement to hatred under Article 137d: 'Anyone who publicly, orally or in writing or image, incites hatred or discrimination against men or violence against person or property on the grounds of their race, religion or beliefs, their gender, their heterosexual or homosexual orientation or their physical, psychological or mental, shall be punished with imprisonment not exceeding one year or fine of the third category.' These Articles satisfy the limitation to the Freedom of Expression under the Dutch Constitution. Moreover, the prescribed law criteria in Article 10 (2) ECHR are also fulfilled.

The ability of the prosecutor to bring charges against those who participate in hate speech can be seen as a way of adequately balancing the Freedom of Expression and protecting against hate speech. The most relevant Dutch cases concern politician Geert Wilders who, after being acquitted of breaching Article 137c and Article 137d of the Dutch Criminal Code in 2011,[1470] was charged and found guilty of breaching said articles after promising that he would take care of an audience's wish for 'fewer Moroccans.' The politician was, however, not fined.[1471]

8.4. Hate speech online

The Netherlands does not have specific legislation governing online environments regarding hate speech.[1472] Instead the general provisions concerning hate speech apply. Online hate speech is hate speech that is disseminated via the Internet, particularly through social media. The Internet brings its own set of difficulties when regulating hate speech. Difficulties include 'anonymity of the person, the rapidness of shared online messages which reach wide ranges of audiences and the fact that messages can be spread transnationally.' Consequently, identifying individuals and enforcing national legislation is more difficult.[1473] This does not however mean that it is impossible to face charges for hate speech in an online environment. The 21 perpetrators who posted online hate speech against politician Sylvana Simons were prosecuted in the following manner: sixteen perpetrators were sentenced to fines

[1470] Rechtbank Amsterdam, 23 juni 2011, ECLI:NL:RBAMS:2011:BQ9001.
[1471] Rechtbank Den Haag, 9 december 2016, ECLI:NL:RBDHA:2016:15014.
[1472] The Swiss Institute of Comparative Law, 'Blocking, filtering and take-down of illegal internet content', 2015.
[1473] Iginio Gagliardone, Danit Gal, Thiago Alves and Gabriela Martinez, Countering Online Hate Speech, (UNESCO series on Internet Freedom, 2015) 8.

ranging from 150 to 450 Euros and four others were sentenced to community service (of 60 to 80 hours).[1474]

8.5. Balance

While there appears to be balance between the Right to Freedom of Expression and its limitations regarding online hate speech, due to, as previously stated, criminalisation under Dutch law, it is vital to note that there is more than one way to find such a balance between the two matters. The European Commission against Racism and Intolerance (ECRI), of the Council of Europe, in its General Policy Recommendations (GPR) No 15, calls for action in several areas to combat hate speech. Areas include raising awareness and prevention; self-regulation; the use of regulatory powers and – as a last resort – criminal investigations and sanctions against hate speech.[1475]

An alternative approach does exist. In the Netherlands online hate speech which is discriminatory in nature can be reported via the Hotline for Discrimination on the Internet (*MiND*). This includes hate speech based on race, religion, disability or sexual preference.[1476] *MiND* assesses the report for criminality and sends a removal request to the website. The message is then deleted from the website.

As a member of the EU, the Netherlands benefits from attempts made by the Union to balance Freedom of Expression and hate speech. According to a 2019 CJEU decision,[1477] platforms, such as Facebook, can be instructed to search for and remove illegal speech worldwide within the framework of the relevant international law. This removal also refers to 'equivalent' content that was previously also declared unlawful. Additionally, in 2016 the Code of Conduct on countering illegal hate speech online was launched by the European Commission with four IT companies (Facebook, Microsoft, Twitter and YouTube).[1478] The Code aims to ensure that requests to remove racist and xenophobic hate speech online are executed rapidly, while simultaneously respecting the fundamental principle of freedom of speech. Companies analyse requests against their

1474 Rechtbank Amsterdam 18 mei 2017, ECLI:NL:RBAMS:2017:3352, ECLI:NL:RBAMS:2017:3343, ECLI:NL:RBAMS:2017:3344, ECLI:NL:RBAMS:2017:3346, ECLI:NL:RBAMS:2017:3347, ECLI:NL:RBAMS:2017:3349; Gerechtshof Amsterdam 15 februari 2018, ECLI:NL:GHAMS:2018:536, ECLI:NL:GHAMS:2018:537, ECLI:NL:GHAMS:2018:538.

1475 ECRI (2019), Fifth Report on the Netherlands CRI(2019)19 < https://rm.coe.int/fifth-report-on-the-netherlands/168094c577> accessed 1 February 2020.

1476 'Over MiND'(Meldpunt Internet Discriminatie (MiND), 2013), <https://www.mindnederland.nl/> accessed 10 February 2020.

1477 C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited (CJEU, 3 October 2019).

1478 There are currently 9 companies which agree to the Code: Facebook, YouTube, Twitter, Microsoft, Instagram, Google+, Dailymotion, Snapchat and Webedia.

community rules and guidelines along with national laws transposing EU law on combating racism and xenophobia.[1479]

8.6. Limitations and Adequacy

About 10% of crimes which contain hate speech, both offline and online, are prosecuted.[1480] Prosecuted cases involving hate speech, both online and offline, tend to include discrimination or the incitement of hatred against a group. The lack of prosecution shows that, while balance between the Freedom of Expression and hate speech is possible, the finding of such a balance is limited and therefore, difficult in practice.

MiND focuses largely on the removal of discriminatory online hate speech. Discrimination is one of the most common forms of hate speech in the Netherlands due to xenophobic views held by an apparently large number of internet users. Consequently, while initiatives of the European Commission are applicable to the Netherlands, it should be noted that the code of conduct is voluntary and thus, not all major IT companies - through which hate speech can be disseminated - follow it. The CJEU decision, C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited, when decided, will, most likely, be very influential in affecting decisions concerning removal of content from online platforms in the Netherlands.

8.7. Conclusion: An inadequate balance

There is no denial that in the Netherlands there are ongoing attempts to balance the freedom of expression and protection against hate speech. However, with such a reliance on the criminal code and, therefore, the prosecution, balance in reality is difficult to achieve. It is no secret that national courts would be unable to process every case based on every complaint ever brought forward to the prosecutor on grounds of online hate speech. As a result, few cases are prosecuted. This method alone is therefore inadequate.

There is no legislation concerning the blocking, filtering and taking-down of illegal internet content. However, there is the presence of the non-governmental *MiND* which receives funding from the Ministry of Justice and Ministry of Social Affairs and Employment. The organisation recognises the importance of the freedom of speech and only requests removal of online posts when the content

[1479] Memo on Code of Conduct on countering illegal online hate speech 2nd monitoring, 1 June 2017, IP/17/1471.

[1480] 'Tolerance and Non-Discrimination Department' (OSCE Office for Democratic Institutions and Human Rights (ODIHR), 2018) <https://hatecrime.osce.org/netherlands> accessed 7 February 2020.

is clearly inciting hatred and violence, i.e. when the content specifically contradicts the criminal code.

Only one national method targeted at balancing the Freedom of Expression online is not enough. Organisations like *MiND* can help provide an adequate balance. Accordingly, the European Commission against Racism and Intolerance (ECRI) has recommended that *MiND* or a similar organisation should be given sufficient funding to monitor the internet systematically for hate speech. Monitoring would include conducting research and building up knowledge on how to trace and eliminate hate speech quickly.[1481] Such a pathway would provide for a better balance between the Freedom of Expression and protection against hate speech online.

9. Has your country reached an adequate balance between allowing Freedom of Expression online and protecting other rights? If not, what needs to be done to reach such a balance?

9.1. General remarks

A succession of clicks and one user. Cyberspace transcends space and time, enabling a user to become the potential starting point of an extended ramification of information through a simple click, reaching multiple receivers. The egalitarian character of Internet Freedom, defined as 'the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection',[1482] empirically translates to a constant flow of information mirroring the diversity of expression, opinions, beliefs and creativity of humankind.

The act of uploading new content online is routine to everyday life. In the last decade, discourse concerning cyberspace and its regulation has given rise to two sides: namely those condemning its arbitrariness and anarchy[1483] versus those romanticising it as a 'domain of pure freedom'[1484] and individual development. Notwithstanding these views, it is of the utmost importance to understand the

[1481] ECRI (2019), Fifth Report on the Netherlands CRI(2019)19 < https://rm.coe.int/fifth-report-on-the-netherlands/168094c577> accessed 1 February 2020, 21.

[1482] Appendix to Recommendation CM/Rec (2016)5 of the Committee of Ministers to member States on Internet freedom, available at <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa#_ftn1> accessed 17 February 2020.

[1483] Jürgen Habermas, Technology and Science as ideology (1st, Beacon Press 1971).

[1484] Julie E Cohen, 'Law for the Platform Economy' (2017) 191, 51 U.C. Davis L Rev 133-204 <https://lawreview.law.ucdavis.edu/issues/51/1/symposium/51-1_Cohen.pdf> accessed 11 February 2020; see also John Perry Barlow, *A Declaration of the Independence of Cyberspace*, (1996), <https://www.eff.org/cyberspace-independence> accessed 11 February 2020.

relevance of cyberlaw in attempting to remedy the Internet's arbitrariness and guarantee legal certainty, publicity and the protection of fundamental rights and freedoms of users. This said task is – usually – carried out within a multi-layered legal framework: involving internet intermediaries, domestic governments and courts and supranational and international legal instruments.

However, as the cyberspace quickly develops, the legislator's task becomes increasingly difficult: on the one hand, new forms of technologies enable hidden cyber threats to individuals' privacy, national security and other fundamental rights; whilst on the other hand, the limited awareness of users and the unprecedented nature of cyberlaw potentially gives governments the opportunity to exercise a patriarchal form of control, thus menacing users' Freedom of Expression online.

This report shall investigate whether the Dutch legal system has been able to strike a balance between Freedom of Expression online and the protection of other rights and shall –accordingly– evaluate possible improvements to this regard.

9.2. Methodology

The following analysis is divided into three parts: the first part concerns the theoretical framework and the legal protection of Internet Freedom in the Dutch legal system. The legal concept of Internet Freedom, as categorised by the EU Recommendation 2016/5, includes:

- The right to freedom of expression online;
- The right to peacefully associate and assembly;
- The right to privacy and family life.[1485]

The second part addresses other fundamental rights that the Dutch legislator must bear in mind when protecting Internet Freedom; this freedom, therefore, not an absolute right. Accordingly, said other rights are going to be structured into three subgroups:

- Good reputation and honour, including the rights to be protected against defamation and false statements;
- Health & morals, including child pornography and revenge porn; online illegal gambling; incitements to violence, hatred and discrimination; illegal drugs and guns related topics. (N.B. hate speech is specifically covered in Report No. 8);

[1485] ibid.

— Intellectual property rights, including copyrights and trademark rights.

In the third and last part of this analysis, the Dutch legal system will be evaluated in light of the balance between Freedom of Expression online and the protection of other rights. Recommendations to the Dutch legal system in this regard will later also be provided. The report is framed using a descriptive approach following a legal doctrinal methodology, providing a final evaluation on the basis of the research outcomes drawn in the main body.

9.3. Internet freedom

Since the written form of Article 19 of the Universal Declaration of Human Rights and of the International Covenant of Civil and Political Rights has come to be, drastic changes have taken place. The inner-need to communicate and express one's mind has driven humans to finding ways of overcoming the two biggest obstacles, namely space and time. After a few decades of legal certainty, both the UN Human Rights Committee and the EU Council have recently highlighted that 'the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice'.[1486]

As many innovative kinds of communication have arisen from cyberspace, the legislator has had to adapt to the new needs of society. It seems the law has facilitated the shaping process of technologies, technologies which are now slowly taking over online governance through voluntary and self-regulating systems.[1487] Therefore, it appears to be the legal responsibility of agencies of state powers[1488] to – again – guarantee the protection of Internet Freedom and acknowledge its wider scope. Accordingly, the first part of this report deals with the legal concept of Internet Freedom and its protection under the Dutch legal system, which is to be framed in the context of European Union law and other relevant international conventions. The approach follows the structure provided by Recommendation CM/Rec (2016)5[1489] of the Committee of Ministers to Member States on Internet freedom, identifying the following elements as integrating elements of Internet Freedom: I. Freedom of Expression online; II The right to peacefully associate and assembly; III. The right to privacy and

[1486] Human Right Committee Resolution A/HRC/38/L.10/Rev.1 on the promotion, protection and enjoyment of human rights on the Internet.

[1487] András Koltay, New Media and Freedom of Expression: Rethinking the Constitutional Foundations of the Public Sphere (Hart Publishing 2019) 66

[1488] Raphael Cohen-Almagor, Confronting the Internet's dark side: moral and social responsibility on the free highway (Cambridge University Press 2015) 53-57.

[1489] ibid.

family life. All these elements contribute to building an enabling environment for Internet Freedom.

9.4. The right to freedom of expression online

This first chapter addresses the primary element of internet freedom, namely the freedom of expression online.

9.4.1. The right to access internet

In 2018, 96.2 percent of the population had access at home to the internet in the Netherlands, 94 percent in Aruba and 87 percent in Curacao (N.B. No complete data for Saint Martin is available).[1490] This data numerically illuminates the expanse of Internet access held by the Dutch population. Encouraging and reinforcing users' democratic engagement in online discourses through access to online information, has also been enhanced by Article 7.4a (1) of the Dutch Telecommunication Act; this national law being the first implementation of the net neutrality principle in Europe.[1491] Under this law, ISP cannot discriminate access to Internet communications on the basis of the user, content, source/destination address, web platform or type of communication. Discrimination is allowed only in so far as it concerns congestion's prevention; security matters; implementation of a legislative provision or court order or transmission to an end-user of unsolicited communication via automated calling and communication systems without human intervention, facsimile machines, or electronic mail.[1492]

Similarly, the European Parliament has approved the Regulation (EU) 2015/2120 laying down measures concerning open Internet access. These match the previous Dutch net neutrality regulations, even though the Dutch parliament has had an extensive debate concerning the 'zero rating' exception, which is allowed under said EU Regulation.[1493]

1490 International Telecommunication Union (ITU), Core House Indicators Report 2019, <https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/CoreHouseholdIndicators.xlsx> accessed 13 February 2020.

1491 For further readings: Nico Van Eijk, "Net Neutrality in the Netherlands" (2014) 7(1) J of Law and Economic Regulation <https://hdl.handle.net/11245/1.445987> accessed 14 February 2020.

1492 Telecommunicatiewet 1998, Articles 7.4a(1) and 11.7(1).

1493 For further readings: Nico Van Eijk, 'Does net neutrality work? The Dutch case' (27th European Regional Conference of the International Telecommunications Society 2016) <https://www.econstor.eu/bitstream/10419/148715/1/van-Eijk.pdf> accessed 14 February 2020.

9.4.1. The freedom of opinion and the right to receive and impart information and the freedom of the media

In the Netherlands, Article 7 of the Civil Code provides for the protection of freedom of media (press, radio and television) and of opinion.[1494] The Dutch legal system is bound by the guidelines framed by the European Convention on Human Rights (hereafter, referred to as: ECHR); Article 10 ECHR recognising the importance of Internet publication in terms of preserving archival material and enhancing access to information[1495]and Article 11 of the EU Charter of Fundamental Rights.

9.4.3. Restrictions and the principle of legality, legitimacy and proportionality

The Dutch legal system does not specifically provide for criteria regarding the restriction of Freedom of Expression online, yet a wide body of case law suggests that local courts[1496] usually follow the three-step test framed in Article 10(2) ECHR. Accordingly, Freedom of Expression online can be limited in so far as there is:

- Legality: a valid legal basis for the occurring restriction;
- Legitimacy: the restriction pursues a goal necessary in a democratic society in the interests of: national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, preventing disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary;
- Proportionality: the legal basis and the particular measure built from it must be necessary, meaning be proportional and correspond to a pressing social need[1497].

N.B. the principle of legitimacy and proportionality thereto is further analysed below under 'Other Rights'.

9.5. The right to peacefully associate and assembly

The act of expressing oneself freely is supported by Article 8 and 9 of the Dutch Constitution, protecting the right of peaceful association and assembly. This

1494 English translation of the Dutch Constitution available at: <https://www.government.nl/search?keyword=constitution+2018&search-submit=> accessed 13 February 2020.

1495 *Times Newspapers Ltd (Nos. 1 and 2) v. the United Kingdom* (2009) ECHR 451.

1496 E.g. ECLI:NL:RBROT:2009:BI1786, District Court of Rotterdam, applying ECtHR affirming that freedom of speech also protects communication that is meant to "offend, shock or disturb".

1497 Handyside v United Kingdom (1976) ECHR App no 5493/72 para 48; Sunday Times v United Kingdom (1979) ECHR App No 6538/74 para 59.

report does not focus on these fundamental rights; however, they must not be entirely neglected, as the increasing role of social media eases the exchange of options and facilitates the physical gatherings of people in civil actions and lawful demonstrations. Interestingly, the Dutch Ombudsman released a report in 2018 expressing a concern towards municipalities and security forces restricting assembly rights for fear of violence and public disorders.[1498]

9.6. The right to privacy and family life

The Netherlands is considered to be one of the freest countries in the world, illustrated by the fact that they have been constantly enhancing the relevance of human rights in international cyber policies since 2013. In its Human Rights Report of 2017, the Ministry of Foreign Affairs has highlighted the complementary relationship between security and the protection of fundamental human rights: such as Freedom of Expression online, privacy and the treatment of personal data.

Despite there being no universal definition, Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights establish the right to privacy, which 'circumscribes the right to protection […] against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons […]'.[1499] In particular, the third cluster of the right to privacy concerns the presumed individual's autonomy over the flow of their personal information and their employment in different contexts.[1500] The new automated means of online data's retention mass surveillance systems have pushed the UN General Assembly towards adopting ten principles,[1501] which – upon publication – shall constitute data protection guidelines for national governments and intergovernmental organisations.

This chapter is going to describe and evaluate whether the Dutch legal system has effectively drawn a balance between the: right to information privacy (I) and the treatment of national security matters (II).

1498 Freedomhouse, Netherlands Freedom Rep 2019 <https://freedomhouse.org/report/freedom-world/2019/netherlands> accessed 16 February 2020.

1499 UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

1500 Jerry Kang, Information Privacy in Cyberspace Transactions (1998) Stanford LR 50 1202–1205.

1501 UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, UN Doc. A/RES/45/95 14 December 1990.

9.7. Privacy and personal data protection: legal framework

Generally speaking, the right to private life is well established by Article 10 of the Dutch Constitution.[1502] Additionally, an amendment to broaden the scope of telecommunications covered by Article 13 of the Dutch Constitution was proposed in July 2017; however, this is yet to enter into force.

The Netherlands is an EU Member State and, as such, is bound by additional legal instruments that come into play in the interpretation and enforcement of privacy and data protection rules. Amongst these, the right to privacy and family life is regulated by Article 8 of the ECtHR case law. Additionally, the right to data protection has been officially recognised as a fundamental right in Article 16(1) of the Treaty on the Functioning of the European Union. Moreover, the Netherlands is also bound by the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108) of the Council of Europe, which has been recently amended in 2019 to add Guidelines covering Artificial Intelligence and Data Protection.[1503]

The Dutch legal system has been deemed as one of the most advanced, in so far as privacy and data protection are concerned. Indeed, prior to the EU General Data Protection Regulation of 2016 (hereafter, referred to as: the GDPR), the Dutch parliament had already signed into law the Data Protection Act (*Wet bescherming persoonsgegevens*). The latter now ceasing to be valid yet appearing, nonetheless, to be very similar to the Dutch GDPR Implementation Act (*Uitvoeringswet Algemene Verordening gegevensbescherming)* (UAVG*)*, which entered into force as of 22 May 2018.

The scope of the UAVG covers all automated data processed by controllers and processors in the Netherlands, except when it relates to criminal investigations; national security or to exclusive journalistic or academic, artistic or literary form of expression purposes.[1504] In all other circumstances, online users' data, processed by controllers and processors, shall comply with the six general data quality principles[1505] and shall satisfy at least one condition for processing

---

1502 English translation of the Dutch Constitution <https://www.government.nl/search?keyword=constitution+2018&search-submit=> accessed 13 February 2020.

1503 Council of Europe Portal, 30 January 2019 <https://www.coe.int/en/web/data-protection/-/new-guidelines-on-artificial-intelligence-and-personal-data-protection> accessed 15 February 2020.

1504 Article 41 UAVG available in Dutch <https://wetten.overheid.nl/BWBR0040940/2018-05-25> accessed 15 February 2020.

1505 Article 5 General Data Protection Regulation 2016/679: "data must be processed fairly and lawfully, collected for specific, explicit and legitimate purposes, adequate, relevant and not excessive, accurate and up to date, kept in an identifiable form for no longer than necessary and, lastly, kept secure" <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 15 February 2020.

personal data, as according to Article 6 of the GDPR.[1506] A breach of data protection is defined by Article 4(12) and shall be notified by controllers to the Data Protection Authority (hereafter, referred to as: DPA) as according to Articles 33 and 34 of the GDPR. Further control is guaranteed by Article 37 GDPR, which obliges controllers and processors to appoint a Data Protection Officer (hereafter, referred to as: the DPO) if they monitor individuals' data on a large scale, or if the data belongs to a special category[1507] or to criminal convictions and offences.

Notwithstanding the GDPR implementation, the Dutch legislator re-established the pre-existing Dutch DPA *(Autoriteit Persoonsgegevens),* which represents the Netherlands in the European Data Protection Board.[1508] The DPA's task is that of supervising the process of personal data in accordance with the GDPR and the UAVG*,* with the additional power of imposing administrative enforcement orders for enforcement purposes. Priority is given to violations that have a big impact on privacy or on minor violations affecting many data subjects, with a special focus on (1) data trading; (2) digital government and (3) artificial intelligence & algorithms.[1509]

Furthermore, personal data is also processed via direct marketing techniques, such as the use of cookies and telecommunications. These are regulated by the Dutch Telecommunications Act, implementing the e-Privacy Regulation, which is yet to be reviewed and amended.[1510] Most notably, pre-ticked checkboxes will no longer be valid consent for the use of cookies, which instead shall require a freely given, specific, informed and unambiguous indication of the data subject

---

1506 Article 6 General Data Protection Regulation 2016/679, available at <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 15 February 2020 :
(a) carried out with the data subject's consent; (b) necessary for the performance of a contract with the data subject; (c) necessary for compliance with a legal obligation; (d) necessary in order to protect the vital interests of the data subject; (e) necessary for the public interest or in the exercise of official authority; or (f) necessary for the controller's or recipient's legitimate interests, except where overridden by the interests of the data subject.

1507 I.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation, financial data, location data, behavioural data and communications data.

1508 Article 6 UAVG <https://wetten.overheid.nl/BWBR0040940/2018-05-25> accessed 15 February 2020.

1509 Autoriteit Persoonsgegevens, Focus AP 2020-2023, available in Dutch <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf> accessed 15 February 2020.

1510 European Data Protection Board (EDPB 2018), Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, available at <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf> accessed 15 February 2020.

through a clear affirmative act.[1511] The supervision of direct marketing and cookies is amongst the tasks of the Dutch Authority for Consumers and Markets *(Autoriteit Consument & Markt)* (ACM), who can impose coercive administrative fines up to 900,000 euros per breach or 10 percent of the annual turnover of the company in breach.[1512]

9.8. Special Circumstances

9.8.1. Data of Minors

Consent from a child to online services is only valid if authorised by a parent. In the Netherlands a child is defined as someone younger than 16 years old.

9.8.2. Data related to serious crimes

Data access that is justified by investigation of suspected serious crimes is regulated by the Dutch Code of Criminal Procedure as well as the Police Data Act and the Judicial Data and Criminal Record Act. Additionally, such investigation always requires the approval of an independent judge or sector-specific regulators.

9.8.3. Data access for national security purposes

Whereas an approval of an independent judge is required for access to personal data for reasons of regular public prosecution, the processing of personal data by the two Dutch secret services (the General Intelligence and Security Service and the Military Intelligence and Security Service) is highly supervised.

9.8.4. Data disclosed for journalistic purposes

The GDPR and UAVG do not apply to disclosure and use of personal data for mere journalistic purposes. In the Satamedia case, the European Court ruled for a broad interpretation of 'journalism', so to also include non-traditional means of communications: covering online bloggers and amateur journalists.[1513] In this circumstance, journalists are presumed to bear a higher responsibility of care towards other privates. The ECtHR has already addressed this legal issue in *Delfi v. Estonia*, where several criteria were taken into account in balancing the right to

---

1511 Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* [2019], <http://curia.europa.eu/juris/document/document.jsf;jsessionid=D6779E745476C38E0BC0A5D481B3608E?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6682950 > accessed 15 February 2020.

1512 Polo van Der Putt et al, 'Data Protection & Cybersecurity 2019' (Chambers and Partners) <https://practiceguides.chambers.com/practice-guides/data-protection-cybersecurity-2019/netherlands> accessed 16 February 2020.

1513 *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* app no 931/13 (ECHR 27 June 2017) paras 53-62.

Freedom of Expression online and the Right to Privacy.[1514] Accordingly, the Dutch legal system approaches these instances case-by-case, whereby special attention is directed towards the consequences following disclosure of personal data, especially if related to negative publications.[1515] Nonetheless, journalists enjoy a higher level of protection under Article 10 ECHR when they proportionally disclose personal data of public authorities (e.g. the police) in the public interest,[1516] fulfilling their role of 'public watchdog'.[1517]

9.8.5. Interpretation, enforcement and executive procedure

The digital age has allowed an egalitarian virtual engagement, which inevitably imparts and allows access to personal information. The monitoring of personal content online allows communication providers and state agencies to observe nearly any act of expression online. This, in turn, negatively impacts the right to Internet freedom.[1518] Accordingly, states' advocacy and support for Freedom of Expression online shall not ignore the implications of the right to privacy and data protection; on this matter, the Dutch privacy and data regulatory framework becomes hugely relevant.

Indeed, the latter only works as long as the enforcement process has been designed and is employed effectively. Notwithstanding the Right to Freedom of Expression online, the publication and use of personal data of another individual – without their consent – leads to the risk of facing legal action. Legal action may concern penalties outlined in (i) concerning DPAs or (ii) concerning civil law claims.

— As for material personal data breaches, the DPA begins investigations upon suspicion or complaint of breaches and accordingly, performs targeted enforcement actions. The principle of proper public administration (i.e. fairness, proportionality and non-discrimination) are guaranteed by the opportunity for the suspected offender: to express their views; to file an objection; to be heard at an oral hearing and to appeal to the District Court and ultimately to the Administrative High Court for Trade and Industry or to the Administrative Jurisdiction Division of the Council of State. Even though the DPA usually imposes administrative orders followed by eventual penalty in case of non-

1514 *Delfi As v. Estonia* app no 64569/09 (ECHR, 16 June 2015) para 83; See further: *Springer v. Germany* appl no 39954/08 (ECHR, 7 February 2012); *Von Hannover v. Germany* (n 2), app nos. 40660/08 and 60641/08 (ECHR, 7 February 2012).

1515 District Court of The Hague, ECLI:NL:RBSGR:2007:BB8427.

1516 ECLI:NL:GHARN:2005:AT0895, Arnhem Court of Appeal.

1517 *Barthold v. Germany*, app no 8734/79 (ECHR, 25 March 1985).

1518 Privacy International, https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression > accessed 16 February 2020.

compliance, the developments in cyber-technologies and the new GDPR case law and upcoming e-Privacy Regulation may lead to further enforcement.

— Individuals may file a civil law claim to: remove personal data (e.g. names, recognisable photos etc.) from the Internet and to refrain from mentioning them again[1519]; request the ISP controller to remove the unlawful publications from their online archive[1520] or to compensate for any material or immaterial damages based on the general Dutch tort provision in Article 6:162 Dutch Civil Code.[1521]

9.9. Surveillance system of national security

Notwithstanding the Dutch efforts in guaranteeing a legal environment balancing human rights and security matters, the entry into force of the Intelligence and Security Services Act *(Wet op de Inlichtingen- en veiligheidsdiensten, Wiv or* ISS Act 2017*)* has been reason for concern amongst human rights foundations and legal academics. The controversial debate has also taken shape through a consultative referendum, which resulted in a negative response towards the new ISS Act. This, however, did not sway the Dutch government from its position, leading to the approval and entry into force of the ISS Act as of 1 May 2018.[1522] Two main concerns, as presented in the IViR Report 2017[1523], are the following:

— Firstly, Article 48 ISS 2017 permits the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) to supervise and intercept bulk cable-bound communications, whereas in the previous ISS 2002 only non-cable bound communications were subjectable to such interceptions.[1524] Any interception must be

[1519] ECLI:NL:RBAMS:2014:1680, District Court of Amsterdam.

[1520] ECLI:NL:RBALM:2012:BY1807, District Court of Almelo.

[1521] Pauline Phoa, Country report the netherlands case study (ii) on freedom of expression in the context of the media (Beucitizens 2016) <https://webcache.googleusercontent.com/search?q=cache:B64gb3NK5qUJ:https://www.uu.nl/en/files/case-study-ii-on-freedom-of-expression-in-the-context-of-the-media-d7-4pdf+&cd=2&hl=it&ct=clnk&gl=nl&client=safari> accessed 17 February 2020.

[1522] Kamerbrief over de Wet op de Inlichtingen- en veiligheidsdiensten, available in Dutch https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/04/25/kamerbrief-over-de-wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv/kamerbrief-over-de-wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv.pdf. > accessed 16 February 2020; see also in Dutch <https://www.parool.nl/nieuws/invoering-sleepwet-uitgesteld-tot-1-mei~b655ba4f/> accessed 16 February 2020.

[1523] IViR, 'Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?' (Utrecht/Amsterdam, March 2018) <https://www.ivir.nl/publicaties/download/Wiv_2017.pdf> accessed 16 February 2020.

[1524] Nicholas Tsagourias et Russell Buchan, Research Handbook on International Law and Cyberspace (Edward Elgar Publoishing, 2015) 225,

directed towards an 'investigation related purpose'; these purposes are determined every four years by the Prime Minister, the Minister of the Interior and Kingdom Relations and the Minister of Defence.[1525] Multiple associations and non-governmental organisations promoting the respect of fundamental human rights have highly criticised the new special power of the AIDV and the MIVD, because it may lead to 'dragnet surveillance' with an insufficient accountability system.[1526] Despite the rejection of a parliamentary motion[1527] expressing these concerns, the government of 2017 addressed the need for further guarantees in the ISS Act 2017, so as to be able to avoid a mass surveillance situation.[1528]

— Secondly, Article 45 ISS 2017 provides the AIVD and MIVD with the new special power to hack into computerised systems and devices, directly or via a third-party device. The latter is a new addition, which enables the gaining of access to targeted devices as such an addition was deemed fundamental and was already the usual practice.[1529] Similarly to the previous concern, a parliamentary amendment addressing subsidiarity and proportionality guarantees was rejected. However, Article 45(5*)* ISS 2017 already excludes hacking into third party devices for surveillance purposes, thus the legislator has already attempted to address an eventual 'dragnet' situation.[1530]

Privacy and data protection have gained the rightful attention of the Dutch legislature, which has now been amended into several legal instruments, namely: The Constitution; the Data Protection Act (now substituted by the UAVG and the GDPR) and the Telecommunications Act. Such legislation ensures a higher and more adequate level of protection within a dynamic and changeable tech-reality. Subsequently, the Netherlands appears to be ahead of most other States and is able to provide its citizens with a considerable level of awareness with regard to their privacy and data protection rights.[1531] This is guaranteed through

<https://books.google.nl/books?id=9ufECQAAQBAJ&lpg=PA225&ots=ypiseX3eIZ&dq=cable%20bound%20communications&hl=it&pg=PA218#v=onepage&q=cable%20bound%20communications&f=false> accessed 16 February 2020.

1525 Article 6 ISS Act 2017.

1526 ibid, 23.

1527 ibid citing Parliamentary Papers II, 2016/2017, 34588, 66.

1528 ibid citing Coalition Agreement 2017 – 2021 VVD, CDA, D66 and Christen Unie, 'Confidence is the Future', 10 October 2017, pg. 4; *Parliamentary Papers* II, 2017/2018, 34588, 69).

1529 ibid citing Parliamentary Papers II, 2016/2017, 34588, 3, pg. 102 and 304.

1530 ibid, 25.

1531 The Netherlands One of the Leaders in Privacy Protection, Leiden University (4 October 2017), <https://www.universiteitleiden.nl/en/news/2017/09/the-netherlands-one-of-the-leaders-in-privacy-protection> archived at <https://perma.cc/QH4Z-TKH3>.

a more severe coercive enforcement of regulations with higher penalties and increasing powers to the relevant supervising authorities (i.e. DPA and ACM*)* and the increasing importance of data breaching notification rules. The Netherlands additionally provides for binding corporate rules for several companies functioning as processors and/or controllers (e.g. ABN AMRO Bank, ING Bank, Rabobank Nederland, Schell International B.V. etc.), in regard to preventing breaches of the GDPR. Furthermore, the Dutch government has also been engaged in informative campaigns in order to raise social sensitivity towards the risks hidden in cyberspace and to promote publicity of the legal instruments that have already been put into place to protect privacy and data protection rights.[1532]

Nonetheless, there is still room for improvement concerning legal certainty and transparency in the collection and processing of personal data and the public engagement of the DPA. In particular, debated topics such as Big Data, Artificial Intelligence and autonomous decision-making devices are not addressed by either the GDPR or by the DPA's guidelines. Furthermore, there is no legal basis providing that special powers to hack into a third-party device are to be employed only when direct access into the targeted system is not possible. Despite this having been clarified by the government during parliamentary debate,[1533] the lack of legal basis inevitably gives more powers to the AIVD and MIVD. As it is recommended that such legal certainty and transparency shall be further addressed in future legal amendments, the protection of fundamental human rights is unbalanced by the complex political and internal accountability required by the ISS 2017 and the duty of care[1534] that shall guide any activity within regular and special powers of both Secret Intelligence Services. As a matter of fact, both the AIVD and MIVD are supervised by the Minister of the Interior and Kingdom Relations and the Minister of Defence and the Secretary-General of the Ministry of General Affairs. Additional accountability of both Secret Intelligence Services is ensured through the required consent from both the minister and the District Court of The Hague, which has been added to comply with the decision in Sanoma Uitgevers B.V,[1535] the decisions in the Telegraph cases,[1536] or the new Review Board.

The balance between political and internal accountability, and the lack of legal certainty and transparency does not lessen the fact that mere perception of

[1532] ibid.
[1533] ibid, 24.
[1534] Article 24 ISS 2017.
[1535] *Sanoma Uitgevers B.V. v The Netherlands* app no 38224/03 (ECHR, 14 September 2010).
[1536] *Telegraaf and Others v. the Netherlands* app no 39315/06 (ECHR, 22 November 2012).

dragnet surveillance may negatively affect the way citizens think of their Right to Freedom of Expression online. This is, indeed, the main concern of various internet respondents, which claim that there is no need for such measures representing unjustified interference in people's fundamental rights.[1537] However, due to the high number of cyber-crimes witnessed in the last years, there is no easy and simple answer to the discourse regarding the balance between the right to privacy and Internet freedom versus national cyber security. Notwithstanding the valid arguments justifying both sides, it is recommended to not take an extremist position and thus, always counterbalance fundamental human rights and nationality security. In this sense, the Netherlands is one of the leading countries in social engagement regarding the output of adequate legal instruments for the protection of the right to privacy and Internet Freedom. Yet, the Dutch government must not neglect the importance of legal certainty, transparency and democratic debate when addressing matters of national security, such as is the case of the ISS of 2017.

9.10. Other Rights

The cyberspace has given human rights and respective violations a new perspective. Article 10(2) ECHR broadly provides limitations to the right to freedom of expression, ranging from the right to privacy and issue of national security (which have already been addressed in Chapter III) to the prevention of health and morals and the protection of reputation or rights of others. In the leading case of *Ahmet Yildirim v. Turkey*,[1538] the ECtHR acknowledged that the Internet has not become a key means of exercising the Right to Freedom of Expression and Information. Accordingly, the principles of legality, legitimacy and proportionality shall be strictly assessed in online cases,[1539] even if states still hold a margin of appreciation in determining what constitutes a pressing social need in their country.[1540]

The following chapters shall each address a possible limitation to the Right to Freedom of Expression in the cyber-perspective, assessing the Dutch approach and the eventual compliance with European and international standards.

9.11. Reputation and Honour: Legal Framework

Internationally, Article 12 UDHR and Article 17 ICCPR protect the right to respect one's reputation and honour. However, this does not justify the severe

---

1537 e.g. Janne E. Nijman and Wouter G. Werner, Netherlands Yearbook of International Law 2018: Populism and International Law (Springer Nature 2019) 283.

1538 *Yildirim v. Turkey* app no 3111/10 (ECHR 18 December 2012).

1539 ibid.

1540 *Mouvement Raëlien v. Switzerland* app no 16354/06 (ECHR [GC] 13 July 2012) para 47.

criminalisation of Internet activities, which has already been condemned by the UN Human Rights Committee.[1541] The latter has especially condemned imprisonment following defamation, which shall be the sentence only in the most severe infringements of fundamental human rights.[1542]

At a European level, this decriminalisation has never been explicitly addressed, but relevant case law has attempted to draw a line in sentencing various forms of defamation.[1543] The right to reputation is implied in Article 8 ECHR, protecting the right to privacy and family life.[1544] The ECHR guidelines on Article 3 put great emphasis on the seriousness test, which is met when the presumed violation infringes the personal enjoyment of the right to respect for private life (both in social and professional spheres).[1545] This seriousness test acquires even more relevance in cases concerning the cybersphere, where commenting underneath someone's else personal content has become a matter of one click. In the context of Internet, the Court distinguishes between content (e.g. including comments) that constitutes 'vulgar abuse' and content of a more trivial nature. Such a distinction is made by considering the circumstances of the case and the importance of the role that the ISP plays in hosting said content within the information society.[1546] Additionally, the Court also takes into account 'the contribution to a debate of general interest; how well known the person concerned is; what the subject of the report is; his or her prior conduct; the method of obtaining the information and its veracity, the content, form and consequences of the publication, and the severity of the sanction imposed'.[1547]

Contrary to the UN recommendation, the Netherlands criminalises all forms of defamation in its Criminal Code in Articles 261(1) (slander*, smaad*), 261(2) (libel, *smaadschrift*), 262 (aggravated defamation, *laster*), 266 (simple insult, *eenvoudige belediging*), 268 (defamatory accusation), 271 (distribution of insulting or slanderous material) and 137c (group defamation based on race, religion or beliefs, sexual orientation or physical, mental or intellectual disability).[1548] All

[1541] General comment No. 34, U.N. Human Rights Committee, 102nd session, published 12 September 2011, available at <www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf> accessed 17 February 2020.

[1542] ibid.

[1543] OSCE, Defamation and Insult Laws in the OSCE Region: A Comparative Study (2017) 7 <https://www.osce.org/fom/303181?download=true> accessed 17 February 2020.

[1544] See e.g. *Axel Springer AG v. Germany* app 39954/08 (ECHR [GC], 7 February 2012) para 83; *Chauvy and Others v. France* app no 64915/01 (ECHR 29 September 2004) para 70.

[1545] *Axel Springer AG v. Germany* app 39954/08 (ECHR [GC], 7 February 2012) para 83.

[1546] *Tamiz v. the United Kingdom* app no 3877/14 (ECHR 19 September 2017) paras 80-90.

[1547] Council of Europe, Guide on Article 8 of the Convention - Right to respect for private and family life (updated 31 August 2019) 37 <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 17 February 2020; see also *Axel Springer AG v. Germany* app 39954/08 (ECHR [GC], 7 February 2012) para 89-95.

[1548] Criminal Code of the Netherlands version 2012

provisions provide a possible imprisonment sentence which, in some cases, may reach two years. Despite the coercive approach of the Dutch legal system, criminal prosecution for defamation is rare and occurs only if the prosecutions would be compatible with the ECtHR, especially when freedom of expression is involved.

9.11.1. Special cases on defamation against public officials, state symbols and institutions

Being a public figure attracts a higher level of personal attention and as a result, said public figure is more likely to be subject to criticism and insults. For this reason, the ECHR Court in *Lingens v. Austria* has advocated for a higher level of tolerance by public figures and state institutions.[1549] Similarly, the UN – together with other international organisations – has called for the repealing of all '*desecato*' laws, especially those providing for custodial sentences.[1550]

Despite the important role that democracy plays in the Netherlands, *lèse-majesté* and '*desecato'* laws are still present in the Dutch legislature. In particular, defamation of a public official or against the State and its symbols is criminalised under Article 267 Dutch Criminal Code. Sanctions for such acts carry a punishment that is a third harsher than for similar acts against another individual. Additionally, defamation against the Head of State and his family may lead to five years of imprisonment and to the eventual loss of civil rights, according to Articles 111, 112 and 114(2) Dutch Criminal Code. Two years of imprisonment is possible under Article 118 Dutch Criminal Code in case of defamation against foreign Heads of States or officials.

According to an OSCE Report,[1551] there have been 255 prison sentences in 2013 for violations of Article 267 on public officials, the State and its symbols and between zero and five convictions for violations of Articles 111-113 (lèse-majesté laws) and Article 118 on foreign heads and officials. Recent cases where defamation was criminalised[1552] did not concern the Right to Freedom of Expression online and the context of the Internet. Additionally, Articles 111-113 and 118 will be repealed by 1 January 2020; this repeal representing the first step towards the decriminalisation of defamation towards public officials.

<http://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf> accessed 17 February 2020.

1549 *Lingens v. Austria* app no 9815/82 (ECHR, 8 July 1986).

1550 Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression (2002)2 7 <https://www.osce.org/fom/99558?download=true> accessed 17 February 2020.

1551 ibid.

1552 ibid, 178.

9.12. Health And Morals

9.12.1. Pornography

Pornography was legalised in the Netherlands in 1986 by Article 240 Criminal Code. Accordingly, in so far as it stays within lawful boundaries, pornography is covered by Article 7 of the Dutch Constitution on Freedom of Expression and by Article 10 ECHR.

9.12.2. Child Pornography

Child pornography constitutes any pornographic material which visually depicts a minor engaged in sexually explicit conduct.[1553] Universally, child pornography is deemed to be illegal.[1554] Subsequently, states are required to provide an adequate legal framework criminalising such activities, especially to protect minors' morals and physical and mental health. This positive duty also flows from Articles 3 and 8 ECHR and the relevant ECtHR case law.[1555]

Accordingly, the Netherlands criminalises the possession, distribution and production of child pornography in Article 240b Dutch Criminal Code. Furthermore, with the rise of internet platforms, the Dutch government has established special cooperation with ISPs in filtering and blocking internet access to child pornography.[1556] To this regard, a blacklist of child pornography is held by the Child Pornography Reporting Office, which is employed by ISPs to filter this type of unlawful content. Lastly, a notice and takedown procedure of child pornography content is possible upon order of the public prosecutor or on voluntary request.[1557]

9.12.3. Revenge Porn

Revenge porn constitutes content of a sexual character that is placed on the Internet without the consent of the person photographed or filmed. The Dutch government has announced its intention to establish a separate crime for revenge porn, which may be punished by a prison sentence of up to two years.[1558] In

---

1553 Council of Europe, Convention on Cybercrime (Budapest 2001) Article 9(2)(a) <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> accessed 17 February 2020.

1554 Article 34 United Nations Convention on the Rights of the Child; Article 9 Council of Europe's Cybercrime Convention; the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

1555 See e.g. *Söderman v. Sweden* app no 5786/08 (ECHR, 12 November 2013).

1556 Government of the Netherlands, 'Sentencing' <https://www.government.nl/topics/crime-and-crime-prevention/sentencing> last accessed 26 February 2020.

1557 Government of the Netherlands, 'Sentencing' <https://www.government.nl/topics/crime-and-crime-prevention/sentencing> last accessed 26 February 2020.

1558 Government of the Netherlands, 'Legislative proposals fortifies approach to crime' <https://www.government.nl/latest/news/2018/11/15/cooperation-and-information-sharing>

relation to the context of the Internet, the District Court of Amsterdam recognised a duty of care that ISPs must respect in regard to hosted user generated content. Accordingly, in one case, the Court held that Facebook must reveal the identity of the 'anonymous and untraceable user' responsible for uploading the unlawful content on the social media platform.[1559]

9.12.4. Online gambling

The Dutch legal system regulates land-based gambling by means of the Betting and Gaming Act 1964 and games of chance by means of the Betting and Gaming Tax Act 1961. Whilst online gambling is still prohibited, the Dutch Senate has approved the Remote Gambling Act in February 2019, authorising commercial operators to exercise interactive betting and gaming online.[1560] Accordingly, further control over online gambling regulations and the Right to Freedom of Expression online is recommended.

9.12.5. Incitement to violence, discrimination and intolerance

N.B. This chapter does not cover the topic of hate speech, despite the relevance thereto, as it is specifically covered in Report No.8.

The Netherlands criminalises acts that incite violence, by Article 131 Dutch Criminal Code. It also criminalises acts that incite hatred or discrimination of a group based on race; religion or beliefs; sexual orientation or physical, mental or intellectual disability by Article 137d Dutch Criminal Code. Furthermore, interpretation and enforcement of these articles is influenced by the ECtHR, which balances the Right to Freedom of Expression online with the protection of other fundamental human rights by means of an assessment of the principles of legality, legitimacy and proportionality, whereby proportionality is met when the restriction is motivated by a pressing social need.[1561]

As for the incitement of violence, the recent *Kaviaar* case[1562] deserves brief attention. In this case, anarchist and pro-refugee poet and activist, Joke Kaviaar, who heavily criticised the immigration policies of Minister Leers, was targeted by the AIVD in the claim that she was inciting public violence and disorder. The legal advisor of Joke Kaviaar invoked Article 10 ECHR and the related cases[1563] including expressions provoking shock, offence and disturbance. In particular,

last accessed 26 February 2020.

1559 ECLI:NL:RBAMS:2015:3984, District Court of Amsterdam.

1560 Kalff Katz et Franssen Attorneys, The Gambling Law Review, 4th ed <https://thelawreviews.co.uk/edition/the-gambling-law-review-edition-4/1194906/netherlands> accessed 17 February 2020.

1561 See e.g. *Leroy v. France* app no 36109/03 (ECHR, 2 October 2008).

1562 ECLI:NL:RBNHO:2013:BY9120, District Court of Harleem.

1563 ibid, para 49.

Kaviaar's legal advisor emphasised the relevance of the client's forms of expressions in the social and democratic debate over asylum and immigration policies. However, the Court of Haarlem considered the contents unlawful and sentenced Kaviaar to four months of prison under Article 131 Dutch Criminal Code. They ruled as such on the basis of the persistent violent nature of the statements and this nature going beyond the limits of the ECtHR. Despite the fact that the texts were taken down in 2011, they are now available both in Dutch and in English[1564] on the webpage of the supporting group '13 September'.

The enforcement and interpretation of Article 131 Dutch Criminal Code on incitement of violence shall follow the guidelines of Article 10 ECHR and related case law. As a matter of fact, the legal defence of Kaviaar, notwithstanding the few public views her texts actually had online, critically refers to the pressing social need for the democratic society behind the restriction and coercive measure taken upon the activist. Whilst the Dutch judicial system is usually in line with ECHR interpretation, the custodial sentence of Joke Kaviaar represents not only a restriction to her personal freedom but may also communicate a new trend in the Dutch Courts, who are adopting a stricter and more patriarchal approach. Yet, Kaviaar remains one case with few comments and thus, more case law is needed to legitimately urge the Dutch legal system to take action to better protect the Right to Freedom of Expression online.

9.13. Intellectual Property

The virtual space represents a unique opportunity to spread forms of expressions through literary, artistic and scientific works of individuals, new products and services of entrepreneurs, databases, inventions, etc. These rights are protected by Article 7 of the Dutch Constitution and Article 10 ECHR. Protection comes in the form of Copyrights, Trademark rights, Patent rights and Database rights; all of which are types of Intellectual Property rights giving the creator of a work the exclusive rights to use, reproduce and/or to exploit the work.

At the European level, the protection of intellectual property rights is implied in the right to property, under Article 1 of Protocol I to the ECHR and related case law. Additionally, the European legislator has addressed liability of ISPs for copyrights violations in Articles 12 and 14 of the e-Commerce Directive;[1565] these articles create a safe harbour for passive ISPs that do not have knowledge of the illegal nature of stored content nor of the circumstances from which this

[1564] Incriminating Joke caviar texts, available at <https://13-september.nl/inciting-texts/> accessed 17 February 2020.

[1565] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce or the e-Commerce Directive).

is apparent. Such addressal by the legislators stating that upon obtaining such knowledge or awareness, ISPs must quickly remove or disable access to the information.

In the Netherlands, the Dutch Copyright Act – together with the Copyright Contract law – aims to protect the original author and their exclusive rights over their work. Additionally, the Dutch government has formulated a Notice and Take down code of conduct in case of copyright infringements. As for trademark rights, they are protected by the Benelux Convention on Intellectual Property, implementing Directive (EU) 2015/2436 (EUTMD) in March 2019.

With the constant flow of information that is cyberspace, it is understandable how intellectual property rights may be at risk. Nonetheless, the balance between the Right to Freedom of Expression and the protection of intellectual property rights is mirrored in the legal framework of copyrights: they are exclusive in so far as limitations do not apply, whereby exceptions are justified by the right to access information and the democratic dissemination of intellectual work. This law was made to handle the clash between the Right to Freedom of Expression online and copyright infringements. To this regard, relevant ECtHR case law has been developed. Indeed, in Ashby Donalds[1566] and The Pirate Bay,[1567] the Court established that a conviction based on copyright rights for illegally reproducing or publicly communicating copyright protected material can be regarded as an interference with the right to freedom of expression by limitations set in Article 10 ECHR. A similar case in the Netherlands is the Dutch BREIN v. Pirate Bay,[1568] which mirrors the judicial approach to content infringing copyrights online. Following the judge's order towards ISP Ziggo and XS4ALL to block a list of 24 websites infringing copyright material relevant to BREIN, the Hague Court of Appeal condemned the non-proportionality of such a measure using, as justification, the right to free entrepreneurship. What is interesting and relevant in this case is the Court's approach in assessing the effectiveness and the contribution of the measure to the democratic society.

As intellectual property is deemed to be the frontier of human rights, concerns arise with the new Article 13 of The European Union Directive on Copyright in the Digital Single Market[1569]; this Article requires online platforms to filter or remove copyrighted material from their websites. The recent character of the new EU Directive does not allow for further evaluation however, the Dutch

1566 *Ashby Donald and others v. France* app no 36769/08 (ECHR,10 January 2013).

1567 *Neij and Sunde Kolmisoppi v. Sweden* app no 40397/12 (ECHR, 19 February 2013 "The Pirate Bay").

1568 ECLI:NL:RBSGR:2007:AZ5678, Court of The Hague.

1569 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

legislator is recommended to bear in mind the importance of fundamental human rights– especially the Right to Freedom of Expression online– when implementing the EU provision into national law.

9.14. Final Evaluation

The first integration element of Internet Freedom[1570] is an enabling environment, where exercising Internet Freedom is free from any illegitimate obstacle. The aim of Part III of this report is to assess whether the Dutch legislator has been able to strike a balance between the Right to Freedom of Expression online and other fundamental rights and, if not, what needs to be done to achieve said goal.

The Netherlands protects human rights and fundamental freedoms on the Internet by means of the general provisions concerning basic rights of the Constitution, such as through Articles 8 through 10, which are valid both off- and online.[1571] In the report, several clashes have been emphasised.

9.14.1. The right to privacy and freedom of expression

The Dutch legal system adheres to the ECHR framework, attributing a higher level of care towards individuals and a more tolerable attitude towards journalists reporting on public figures. The legal framework is advanced towards digital rights, even if topics like artificial intelligence and Big Data are yet to be addressed.

9.14.2. The right to privacy, Internet freedom and national security

The right to privacy in the Netherlands is threatened by a new global trend of mass surveillance, which, in the Netherlands, took shape through the ISS Act 2017. The latter presents issues concerning transparency, accountability and legal certainty, especially with regard to hacking and interceptions of bulk cable-bound communications.

9.14.3. Freedom of expression online and the right to reputation

The Netherlands provides adequate legal basis for the protection of the right to reputation, which holds both offline and online. However, a negative outbalance is represented by the severe custodial sentences for defamation of public officials and state symbols and institutions; this is not in line with international standards of democratic practices. Yet, recent efforts to repeal *lèse-majesté* laws by 1 January 2020 suggest that the Dutch government is on the right path.

[1570] ibid.
[1571] ibid.

9.14.4. Freedom of expression online and pornography (child pornography and revenge porn)

The Dutch government has repeatedly shown efforts and will to provide minors and, more generally, vulnerable citizens more protection from child pornography and revenge porn, positively balancing out the Right to Freedom of Expression online.

9.14.5. Freedom of expression online and online gambling

The clash between online gambling and the Right to Freedom of Expression online has abstractly arisen from the recent Remote Gambling Act, adopted in February 2019. Further research on related cases is needed in order to assess whether the legislator has been able to draw a balance between the Right of Freedom of Expression online and the protection of health and morals online.

9.14.6. Freedom of Expression online and incitement to violence, discrimination and intolerance

Generally, the Dutch legal framework adheres to the ECHR interpretation and guidelines. Further oversight is recommended with regard to national Courts' interpretation of 'pressing social need' and eventual coercive sentences thereto.

9.14.7. Freedom of Expression online and intellectual property right (Copyright and Trademark)

The Netherlands guarantees the protection of copyrights, whilst still guaranteeing the Right to Freedom of Expression online according to the ECtHR. However, Article 13 of the new Copyright Directive is concerning and research into the Dutch implementation and enforcement is recommended.

In brief, the Netherlands is one of the leaders in promoting the Right to Freedom of Expression online and, as drawn from the research outputs of this report, in counterbalancing Internet Freedom with the protection of other fundamental rights. Further research and oversight are recommended with regard to the new implementation and enforcement of Article 13 of The European Union Directive on Copyright in the Digital Single Market, the eventual address of artificial intelligence and Big Data by domestic and/or EU legal instruments, the enforcement of the ISS 2017 Act – especially with regard to hacking and interceptions of bulk cable-bound communications – and *'desecato'* laws criminalising defamation towards public officials, state symbols and institutions.

10. How do you rank (1-5) the access to freedom of expression online in the Netherlands?

As the global economy has grown, the issue of protecting the freedom of expression - online and offline - has become more crucial. This is because it is considered to be a vital element to the functioning of a democratic society.[1572]

The Netherlands has always been keen to foster internet freedom worldwide. Even back in 2011, the Foreign minister Uri Rosenthal said that freedom of expression must be guaranteed, including on the internet. Consequently, the Netherlands is working internationally to uphold internet freedom so that cyber-dissidents can receive information and express their views on the internet without fear of reprisals.[1573] Therefore, the Netherlands would have a mark 5 out of 5 concerning the access to freedom of expression online.

That being said, the media in the Netherlands remains open, accessible, and diverse– operating in one of the freest environments in the world. To compare, this is hugely different to China where 'censorship [has] reached unprecedented extremes' according to The Freedom House. Freedom of expression in the Netherlands is protected by Article 7 of the Dutch Constitution and Article 10 of the European Convention on Human Rights (hereafter referred to as: the ECHR).[1574] The scope of protection covers expression to the extent that it does not contradict the fundamental values of the ECHR.

It is vital to note that the Netherlands made online human rights one of the pillars of its international cyber policy of the International Cyber Strategy. The Netherlands deems security and freedom as essentially complementary interests. It is evident that universal human rights – such as freedom of expression, freedom of information, the right to privacy and the protection of personal data – should be respected online as well as offline.[1575]

In spite of this, the above-mentioned freedoms are increasingly threatened online. The ability of state actors to suppress dissident voices online is growing. In addition, governments increasingly hack the accounts of human rights defenders, as well as deploying advanced intimidation techniques and censorship towards these people. The tactics of blocking access to the Internet and deliberately spreading false information, or of using the fight against

[1572] Nowak M., 'An Introduction to International Human Rights Regime', Nijhoff, 2003.
[1573] ibid.
[1574] Grondwet [Constitution], 24 August 1815, Staatsblad van het Koninkrijk der Nederlanden [Stb.] [Official Gazette of the Kingdom of the Netherlands] 1815, No. 45; European Convention on Human Rights [ECHR], 4 November 1950, 213 U.N.T.S. 221.
[1575] Ministry of Foreign Affairs (2018), International human rights policy: activities and results, Human Rights Report, 2018.

disinformation to exercise censorship and violate privacy, have become increasingly common in the last year.[1576] The Netherlands speaks against such practices and uses both financial and diplomatic means to help human rights defenders arm themselves against such measures.[1577]

Since 2012, the Netherlands has been helping to develop an international normative framework for strengthening human rights online – particularly the right to freedom of expression. The Netherlands opposes attempts to restrict human rights online on the basis of the misguided assumption that increased internet usage constitutes a danger.

All things considered, Freedom of Expression in the Netherlands is apparent despite concerns related to the adoption of stricter online regulations. The media and civil society frequently discuss the state of internet freedom in the Netherlands openly; internet regulation issues are often given great prominence in widely read online news publications. An independent court system provides oversight of regulatory measures adopted by the executive and the legislature.[1578]

The Dutch Government ensures that Freedom of Expression is a top priority for various international organisations, including the United Nations; the Organization for Security and Co-operation in Europe and the European Union. Furthermore, the Netherlands effectively works with non-governmental organisations that promote freedom of expression, such as the Free Press Unlimited and RNW Media. The Netherlands, thus, frequently draws attention, at both a bilateral and multilateral level, to the importance of keeping the internet open, free and safe.

Together with eight other countries from the Freedom Online Coalition (FOC), the Netherlands has supported the Digital Defenders Partnership (DDP) since 2016. An evaluation of the programme in 2017 yielded a favourable assessment. The FOC adopted a statement on internet censorship in 2018. The Netherlands successfully called for the inclusion of a definition of internet censorship in order to prevent the statement from being misused. The statement has since been used as a point of reference for the drafting of new resolutions in a multilateral context.

Over the last few years, the Netherlands has devoted particular attention to network shutdowns: a collective term for measures taken by governments to

---

1576 Adrian Shahbaz, The Rise of Digital Authoritarianism, Freedom of the Net 2018 (2018). <https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf>.

1577 Romano, A. (2009). Public Sentinel: News Media and Governance Reform. (P. Norris, Ed.) World Bank Publications.

1578 Ministry of Foreign Affairs (2018), "nternational human rights policy: activities and results, Human Rights Report, 2018.

restrict internet access and functionality. Examples of such measures include closing off parts of the internet; making websites and social media platforms, like Facebook, inaccessible and blocking messaging apps, like WhatsApp. The Netherlands has openly spoken against such disruptive measures in bilateral meetings and at multilateral conferences.

Protection and promotion of human rights online are embedded in Dutch human rights policy through their International Cyber Policy (Parliamentary Paper 26 643, no. 447). The basic principle of said policy is that the Netherlands regards freedom and security not as opposing interests, but rather as mutually reinforcing. Universal human rights apply both online and offline, with a particular emphasis on freedom of expression, free access to information, privacy and the protection of personal data.

In 2018 the issue of online disinformation came to occupy a prominent place in the political agendas of the Netherlands, the EU and beyond. Online disinformation can present a real threat to trust in government and thus, within the democratic process. Addressing this threat requires a considered response from the government. In 2019, the Netherlands made efforts to highlight this principle both within and outside of the EU.

11. How do you overall assess the legal situation in the Netherlands regarding internet censorship?

Access to online content in the Netherlands is mostly free. Pressure on social media companies to remove illegal content from their platforms, however, has intensified over the past years with the passing of the EU Copyright Directive. Users, notably young users, harnessed online tools to mobilise for social causes – including, for example, the call for action to address climate change. Another protest movement organised largely online opposed said EU Copyright Directive.[1579] Despite this, the Dutch government rarely engages in blocking of websites or internet content. All major social media platforms and international blog-hosting services are freely available.[1580]

The Netherlands has a long tradition of freedom. In keeping with this tradition, Dutch human rights policy focuses on the ability to express oneself. The Dutch government has raised the Human Rights Fund budget by €5.4 million in 2018,

[1579] Cortés, M., Internet censorship around the world, 2000. Retrieved from <http://www.isoc.org/inet2000/cdproceedings/8k/8k_4.htm> accessed 25 February 2020.

[1580] Wimmer, R., & Dominick, J. (2011). Mass media research: An introduction (9th ed.). Belmont, CA: Thompson Wadsworth.

and thereafter by €9.6 million in 2019. An additional reason for such inflated funding, is that better national observance of human rights allows for a more secure society which achieves higher rates of economic growth. The legal situation in the Netherlands concerning internet censorship is thus regulated on national as well as EU level.[1581]

Although the internet is free, there are some restrictions on the promotion of illegal materials. Such can be seen in the case of *Stichting BREIN* where the Dutch antipiracy organisation had won a court case against the file-sharing website Pirate Bay. The CJEU passed its judgment in this case, maintaining that the making available and management of a website on which user-submitted torrent file links to copyright works are indexed, may constitute copyright infringement. Although the protected works were not hosted by the Pirate Bay website, – they were hosted by its users through a peer-to-peer network – the operators, nonetheless, played an essential role in making said works available. The operators had full knowledge of what they were facilitating as evident in the fact that they checked whether works were placed in the appropriate category, deleted obsolete or faulty torrent files and actively filtered some content.[1582]

Government mandated Internet censorship is non-existent due to the Dutch House of Representatives speaking against online filtering on multiple occasions, despite there having been some exemptions with regard to child pornography as in 2008 the Minister of Justice proposed a plan to block websites known to contain child pornography. A blacklist created by the Hotline combating Child Pornography on the Internet (*Meldpunt ter bestrijding van Kinderpornografie op Internet*) (MiND)[1583] would have been used by Internet service providers to redirect websites, containing such pornography, to a stop page. However, the plan was withdrawn due to an 'almost complete lack of websites to block' because the sharing of the material was not done by conventional websites, but by other services.[1584] The House of Representatives reaffirmed this by voting against the proposed filter system later that year, effectively eliminating any plans for government censorship.[1585]

In a consultative referendum held in March, many voters rejected the controversial Intelligence and Security Services Act passed by the parliament in 2017; this act gave the government sweeping powers to access telephone and

---

[1581] ibid.

[1582] Case C-610/15 CJEU Judgment Stich*ting Brein v. Ziggo BV and XS4All Internet BV* (2017) ECLI:EU:C:2017:456.

[1583] Rene Schoemaker, WebWereld (IDG Netherlands), 7 March 2011.

[1584] ibid.

[1585] Joost Schellevis, "Politics says no to internet filter" Tweakers, 18 May 2011.

internet records. Such powers incited criticism of voters, who stated that this could enable surveillance of private communications. Despite the referendum results, the law entered into force in May 2018. Moreover, the Netherlands has had *lèse majesté* laws, which forbid insulting the monarchy in place since 1881.[1586]

In 2019, the European Parliament passed a regulation aimed at 'tackling the dissemination of terrorist content online.' Such tackling would require platforms to delete content of this threatening nature within one hour of receiving a removal order from authorities.[1587] Platforms that routinely fail to do so could be fined four percent of their overall annual revenue. The resolution has, however, not yet entered into force because it must first be approved by other EU bodies. In March 2017, Facebook, Microsoft, Twitter and YouTube launched the prototype of an upload filter based on a shared database to suppress terrorist and extremist content.[1588] In March 2018, the European Commission recommended that social media platforms should expedite and broaden this approach.[1589]

In March 2019, the European Parliament passed the Directive on Copyright,[1590] which imposed a so-called 'link tax'; this 'tax' granting online publishers the right to charge aggregators – i.e. Google News – for excerpting proprietary content, for example, news articles. The directive also makes content-hosting and sharing-platforms, such as YouTube, liable for copyrighted material uploaded by users.[1591]

The search engine delisting process facilitated under the right to be forgotten follows guidelines developed by an advisory group of experts, aiming to strike a balance between the right to be forgotten on the one hand, and Freedom of Expression and information on the other.[1592] Under the new General Data Protection Regulation (GDPR), the Right to be Forgotten is now part of codified data protection law across the EU.[1593]

1586 Wetboek van Strafrecht [Dutch Criminal Code], 3 March 1881, Stb. 1881, No. 35.

1587 European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)).

1588 Matthias Monroy, "Facebook, Twitter & Co: Upload-Filter gegen 'Terrorismus und Extremismus' gestartet" [Facebook, Twitter, and co.: upload filter against 'terrorism and extremism' activated], Netzpolitik.org, March 13, 2017.

1589 Holger Bleich, (2018). "EU demands online platform upload filter immediately", Heise.

1590 Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market COM/2016/0593 final - 2016/0280 (COD).

1591 ibid.

1592 Eco.de, "One year right to be forgotten: Removal of search results impairs civil society", May 13, 2015.

1593 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 17.

Table of legislation

Provision in Dutch language	**Translation in English**
Auterswet, Article 25d De maker kan in rechte een aanvullende billijke vergoeding vorderen van zijn wederpartij, indien de overeengekomen vergoeding gelet op de wederzijdse prestaties een ernstige onevenredigheid vertoont in verhouding tot de opbrengst van de exploitatie van het werk. Indien de ernstige onevenredigheid tussen de vergoeding van de maker en de opbrengst van de exploitatie van het werk is ontstaan nadat het auteursrecht door de wederpartij van de maker aan een derde is overgedragen, kan de maker de vordering als bedoeld in het eerste lid tegen de derde instellen.	Copyright Act, Article 25d The creator can claim additional equitable compensation from the counterparty if, in view of the mutual performance, the agreed compensation is seriously disproportionate to the proceeds from the exploitation of the work. If the serious disproportion between the compensation of the creator and the proceeds from the exploitation of the work arose after the copyright of the creator has been transferred to a third party, the creator can claim towards the latter the same as referred to in the first paragraph.
Auteurswet, Article 26d De rechter kan op vordering van de maker, tussenpersonen wier diensten door derden worden gebruikt om inbreuk op het auteursrecht te maken, bevelen de diensten die worden gebruikt om die inbreuk te maken, te staken.	Copyright Act, art 26d The judge may, on request of the maker, order the intermediary, whose services are used by third parties to infringe copyright, to cease the services used to infringe that copyright.
Burgerlijke Wetboek, Article 6:162 Hij die jegens een ander een onrechtmatige daad pleegt, welke hem kan worden toegerekend, is verplicht de schade die de ander dientengevolge lijdt, te vergoeden. Als onrechtmatige daad worden aangemerkt een inbreuk op een recht en een doen of nalaten in strijd met een wettelijke plicht of met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, een en ander behoudens de aanwezigheid van een rechtvaardigingsgrond. Een onrechtmatige daad kan aan de dader worden toegerekend, indien zij te wijten is aan zijn schuld of aan een oorzaak welke krachtens de wet of de in het verkeer geldende opvattingen voor zijn rekening komt.	Dutch Civil Code, Article 6:162 A person who commits a tortious act (unlawful act) against another person that can be attributed to him, must repair the damage that this other person has suffered as a result thereof. As a tortious act is regarded a violation of someone else's right (entitlement) and an act or omission in violation of a duty imposed by law or of what according to unwritten law has to be regarded as proper social conduct, always as far as there was no justification for this behaviour. A tortious act can be attributed to the tortfeasor if it results from his fault or from a cause for which he is accountable by virtue of law or generally accepted principles (common opinion).

Burgerlijke Wetboek, Article 196c (4) Degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3, bestaande uit het op verzoek opslaan van van een ander afkomstige informatie, is niet aansprakelijk voor de opgeslagen informatie, indien hij: niet weet van de activiteit of informatie met een onrechtmatig karakter en, in geval van een schadevergoedingsvordering, niet redelijkerwijs behoort te weten van de activiteit of informatie met een onrechtmatig karakter, dan wel zodra hij dat weet of redelijkerwijs behoort te weten, prompt de informatie verwijdert of de toegang daartoe onmogelijk maakt.	Dutch Civil Code, Article 196c (4) A person who provides a service of the information society as meant in Article 3:15d, paragraph 3, of the Civil Code, consisting of the storage of information provided by a recipient of the service, is not liable for the information that is stored at the request of a recipient of the service, on condition that the provider: does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or; upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
Burgerlijke Wetboek, Article 196c (5) Het hiervoor bepaalde staat niet in de weg aan het verkrijgen van een rechterlijk verbod of bevel.	Dutch Civil Code, Article 196c (5) The above mentioned paragraphs do not affect the possibility to get a court order to terminate or prevent an infringement or an injunction for the removal or disabling of access to information.
Grondwet, Article 7 Niemand heeft voorafgaand verlof nodig om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet. De wet stelt regels omtrent radio en televisie. Er is geen voorafgaand toezicht op de inhoud van een radio- of televisieuitzending. Voor het openbaren van gedachten of gevoelens door andere dan in de voorgaande leden genoemde middelen heeft niemand voorafgaand verlof nodig wegens de inhoud daarvan, behoudens ieders verantwoordelijkheid volgens de wet. De wet kan het geven van vertoningen toegankelijk voor personen jonger dan zestien jaar regelen ter bescherming van de goede zeden. De voorgaande leden zijn niet van toepassing op het maken van handelsreclame.	Dutch Constitution, Article 7 No one shall require prior permission to publish thoughts or opinions through the press, without prejudice to the responsibility of every person under the law. Rules concerning radio and television shall be laid down by Act of Parliament. There shall be no prior supervision of the content of a radio or television broadcast. No one shall be required to submit thoughts or opinions for prior approval in order to disseminate them by means other than those mentioned in the preceding paragraphs, without prejudice to the responsibility of every person under the law. The holding of performances open to persons younger than sixteen years of age may be regulated by Act of Parliament in order to protect good morals. The preceding paragraphs do not apply to commercial advertising.

Grondwet, Article 8 Het recht tot vereniging wordt erkend. Bij de wet kan dit recht worden beperkt in het belang van de openbare orde.	Dutch Constitution, art 8 The right to association is recognised. This law can be limited by law in the interest of public order.
Grondwet, Article 9 Het recht tot vergadering en betoging wordt erkend, behoudens ieders verantwoordelijkheid volgens de wet De wet kan regels stellen ter bescherming van de gezondheid, in het belang van het verkeer en ter bestrijding of voorkoming van wanordelijkheden.	Dutch Constitution, Article 9 The right to a meeting and demonstration is recognised, subject to everyone's responsibility under the law The law may lay down rules for the protection of health, in the interest of traffic and in the interests of traffic combating or preventing disorder.
Grondwet, Article 10 Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.	Dutch Constitution, Article 10 Everyone has the right to respect for his or her privacy, subject to restrictions imposed by or pursuant to the law. The law sets rules for the protection of privacy with regard to the recording and providing of personal data. The law lays down rules with regard to the claims of individuals for access to information recorded about them and for the use made of it, as well as for the improvement of such information.
Grondwet, Article 71 De leden van de Staten-Generaal, de ministers, de staatssecretarissen en andere personen die deelnemen aan de beraadslaging, kunnen niet in rechte worden vervolgd of aangesproken voor hetgeen zij in de vergaderingen van de Staten-Generaal of van commissies daaruit hebben gezegd of aan deze schriftelijk hebben overgelegd.	Dutch Constitution, Article 71 Members of the States General, Ministers, State Secretaries and other persons taking part in deliberations may not be prosecuted or otherwise held liable in law for anything they say during the sittings of the States General or of its committees or for anything they submit to them in writing.
Grondwet, art 93 Bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties, die naar haar inhoud een ieder kunnen verbinden, hebben verbindende kracht nadat zij zijn bekendgemaakt.	Dutch Constitution, Article 93 Provisions of treaties and of resolutions by international institutions which may be binding on all persons by virtue of their contents shall become binding after they have been published.
Mediawet, Article 8.1 Er is een Stimuleringsfonds voor de journalistiek.	Media Act, Article 8.1 There is a Stimulation Fund for journalism.

Het Stimuleringsfonds heeft rechtspersoonlijkheid en is gevestigd in de gemeente 's-Gravenhage.	This Stimulation Fund has a legal personality, and it is established in the municipality of 's-Gravenhage.
NTD Gedragscode, Article 1 Deze code richt zich op een procedure voor tussenpersonen voor het omgaan met meldingen van onrechtmatige en strafbare inhoud op Internet. De code richt zich op tussenpersonen die in Nederland een openbare (telecommunicatie) dienst op Internet leveren. Deze code is niet van toepassing op situaties waar voor tussenpersonen op basis van wetgeving en jurisprudentie andere verplichtingen gelden.	NTD Code of Conduct, Article 1 This code establishes a procedure for intermediaries to deal with reports of unlawful content on the Internet. The code is provided for intermediaries that provide a public (telecom-munications) service on the Internet in the Netherlands. This code is not applicable to situations in which other statutory obligations or liabilities apply for intermediaries on the basis of legislation and juri-sprudence.
NTD Gedragscode, art 2 Een melding betreft het door een melder aan een tussenpersoon melden van (vermeende) onrechtmatige of strafbare inhoud op Internet met als doel deze inhoud van Internet te laten verwijderen. De melder is de persoon of instantie die een melding doet. De inhoudsaanbieder is de persoon (of instantie) die bepaalde (gewraakte) inhoud op Internet heeft gezet. Een tussenpersoon is de aanbieder van een (telecommunicatie) dienst op Internet. Een controle- of opsporingsdienst is een daartoe bij of krachtens de wet aangewezen overheidsdienst die een algemene of bijzondere opsporingsbevoegdheid heeft.	NTD Code of Conduct, Article 2 A report concerns the reporting by a notifier of (alleged) unlawful content on the Internet to an intermediary with the objective of having this content removed from the Internet. The notifier is a person or organisation that makes a report. The content provider is the person (or organisation) that has placed (contested) content on the Internet. An intermediary is the provider of a (telecommunications) service on the Internet. An inspection or investigation service is a legally appointed governmental service that has general or particular powers of investigation
NTD Gedragscode, art 3 Tussenpersonen hebben een eigen, openbaar toegankelijke Notice-and-Take-Down procedure in overeenstemming met deze code. Deze procedure beschrijft hoe door tussenpersonen om wordt gegaan met meldingen van strafbare of onrechtmatige inhoud op Internet. Met behulp van deze procedure willen tussenpersonen bereiken dat een melding altijd afgedaan wordt en dat strafbare en/of onrechtmatige inhoud van Internet verwijderd wordt. Een tussenpersoon publiceert een procedure waarin beschreven staat op welke wijze en binnen welke termijnen meldingen door de tussenpersoon afgehandeld worden. Binnen	NTD Code of Conduct, Article 3 Intermediaries have their own Notice-and-TakeDown procedure that the public must be able to consult and that is consistent with this code. This procedure describes how intermediaries deal with reports of unlawful content on the Internet. By means of this procedure, intermediaries wish to ensure that a report is always dealt with and that unlawful content is removed from the Internet. An intermediary public-shes a procedure in which the manner and within which time limits reports are dealt with by the intermediary. Distin-ctions can be made

deze procedure kan onderscheid gemaakt worden tussen verschillende vormen van dienstverlening. Een tussenpersoon kan gebruiksvoorwaarden publiceren binnen haar dienstverleningsovereenkomst waarin criteria zijn vermeld wanneer er volgens de tussenpersoon sprake is van ongewenste inhoud.	between various different forms of service provision within this procedure. An intermediary can publish conditions of use within its service provision agreement in which criteria state what constitutes undesirable content in the view of the intermediary.
NTD Gedragscode, art 4 Een melding wordt bij voorkeur pas gedaan nadat aannemelijk is dat de melder en de inhoudsaanbieder niet tot overeenstemming (kunnen) komen. De melder is verantwoordelijk voor het doen van juiste en vol- ledige meldingen. Meldingen in het kader van een opsporingsonderzoek betreffende een strafbaar feit moeten voor de tussenpersoon verifieerbaar afkomstig zijn van een controle- of opsporingsdienst, of – in geval van een wettelijk bevel – van de Officier van Justitie. Voor overige dan in artikel 4a genoemde meldingen geeft de melder in ieder geval de volgende gegevens: contactgegevens van de melder; de gegevens die de tussenpersoon nodig heeft om de inhoud te kunnen beoordelen, waaronder ten minste de locatie (URL); beschrijving waarom de inhoud volgens de melder onrechtmatig of strafbaar is of waarom deze volgens de melder strijdig is met door de tussenpersoon gepubliceerde criteria ten aanzien van ongewenste inhoud; motivering waarom deze tussenpersoon wordt benaderd als meest geschikte tussenpersoon om op te treden. Een melder kan de tussenpersoon verzoeken de melding met spoed af te handelen. Dit dient voldoende gemotiveerd te worden door de melder. Op basis van de motivering bepaalt de tussenpersoon of een spoedprocedure wordt toegepast. Een tussenpersoon kan een melder om een expliciete vrijwaring verzoeken tegen aanspraken van de inhoudsaanbieder ten gevolge van het nemen van maatregelen ter afhandeling van de melding.	NTD Code of Conduct, Article 4 It is preferable that a report is only made once it is likely that the notifier and the content provider will be unable to reach an agreement. The notifier is responsible for ensuring reports are correct and complete. The intermediary must be able to verify that reports as part of an investigation regarding a criminal offence have originated from an inspection or investigation service, or – in the case of a formal legal order – from the Public Prosecutor's Office. For reports other than those stated in Article 4a, the notifier in any case provides the following information: the contact details of the notifier; the information that the intermediary needs to be able to evaluate the content, at least including the location (URL); a description of why the content is unlawful according to the notifier, or why it is in conflict with the criteria published by the intermediary governing undesirable content; a statement of the reason why this intermediary is being approached as the most appropriate intermediary to deal with the matter. A notifier can request that the intermediary deals with the report as a matter of urgency. The reasons for this should be fully explained by the notifier. The intermediary determines whether the report is dealt with as a matter of urgency on the basis of the explanation of the reasons. An intermediary can request an explicit indemnity from a notifier against claims from the content provider as a result of taking measures in the context of dealing with the report.

NTD Gedragscode, art 5 Na ontvangst van een melding wordt deze door de tussenpersoon conform diens eigen procedure behandeld. Meldingen zoals bedoeld in artikel 4a betreffen strafbare inhoud. Van meldingen zoals bedoeld in artikel 4b maakt een tussenpersoon een beoordeling om te bepalen of er sprake is van onmiskenbare onrechtmatigheid en/of strafbaarheid.	NTD Code of Conduct, Article 5 On receipt of a report it is dealt with by the intermediary according to the intermediary's own procedure. Reports as referred to in Article 4a concern punishable content. An intermediary evaluates reports as referred to in Article 4b to determine whether they are unequivocally unlawful and/or punishable
NTD Gedragscode, art 6 De tussenpersoon onderneemt actie op basis van de uitkomsten van het beoordelingsproces. Indien er volgens de tussenpersoon geen sprake is van onmiskenbaar onrechtmatige en/of strafbare inhoud stelt de tussenpersoon de melder hiervan op de hoogte en motiveert dit. Indien er volgens de tussenpersoon sprake is van onmiskenbaar onrechtmatige en/of strafbare inhoud dan zorgt de tussenpersoon ervoor dat de betreffende inhoud onverwijld verwijderd wordt. Indien niet tot een eenduidig oordeel wordt gekomen of er al dan niet sprake is van onrechtmatige en/ of strafbare inhoud, dan stelt de tussenpersoon de inhoudsaanbieder op de hoogte van de melding met het verzoek de inhoud te verwijderen of contact op te nemen met de melder. Indien de melder en de inhoudsaanbieder er niet uitkomen, kan de melder overgaan tot het doen van aangifte als hij of zij meent dat het om een strafbaar feit gaat. Gaat het om vermeende onrechtmatige inhoud, dan moet de melder bij voorkeur in staat worden gesteld zijn geschil met de inhouds-aanbieder voor de rechter te brengen. Indien de inhoudsaanbieder zich niet bekend wil maken aan de melder, kan de tussenpersoon overgaan tot het verstrekken van NAW-gegevens van de inhoudsaanbieder aan de melder of tot het verwijderen van de betreffende inhoud. Teneinde te voorkomen dat bij de door de tussenpersoon te nemen maatregelen méér inhoud dreigt te worden verwijderd dan waarop de melding betrekking heeft, neemt	NTD Code of Conduct, Article 6 The intermediary takes action on the basis of the results of the evaluation process. In the event that the intermediary determines that the content concerned is not unequivocally unlawful, the intermediary informs the notifier accordingly, together with the reasons for this. In the event that the intermediary determines that the content concerned is unequivocally unlawful, the intermediary ensures that the content concerned is immediately removed. In the event that it has not been possible to come to an unequivocal judgement as to whether the content concerned is unlawful, the intermediary informs the content provider about the report with the request to remove the content or to contact the notifier. If the notifier and the content provider are unable to reach an agreement, the notifier can choose to make an official report to the police if in his or her opinion it concerns a criminal offence. If it concerns content that is alleged to be unlawful under civil law, it is preferable that the notifier is able to bring his or her dispute with the content provider before the courts. Should the content provider be unwilling to make him or herself known to the notifier, the intermediary can decide to provide the notifier with the content provider's name and contact details or to remove the content concerned. The intermediary exercises due caution in the execution of the measures that have to be taken to ensure that the removal of any

de tussenpersoon de nodige zorgvuldigheidseisen in acht.	more content than that to which the report refers is avoided.
Politiewet, Article 2 Ambtenaren van politie in de zin van deze wet zijn: ambtenaren die zijn aangesteld voor de uitvoering van de politietaak; ambtenaren die zijn aangesteld voor de uitvoering van technische, administratieve en andere taken ten dienste van de politie; vrijwillige ambtenaren die zijn aangesteld voor de uitvoering van de politietaak, onderscheidenlijk voor de uitvoering van technische, administratieve en andere taken ten dienste van de politie; ambtenaren van de rijksrecherche die zijn aangesteld voor de uitvoering van de politietaak, onderscheidenlijk voor de uitvoering van technische, administratieve en andere taken ten dienste van de rijksrecherche.	Police Act, Article 2 Police officers within the meaning of this Act are: officials appointed to carry out the police tasks; officials appointed to perform technical, administrative and other duties at the service of the police; voluntary officials appointed to perform the police task or to perform technical, administrative and other duties at the service of the police; civil servants of the Department of Criminal Investigation who are appointed for the execution of the police task, respectively for the execution of technical, administrative and other tasks at the service of the Department of Criminal Investigation.
Telecommunicatiewet, Artikrl 7.4 Aanbieders van openbare telefoondiensten op een vaste locatie of van openbare betaaltelefoons die krachtens artikel 9.2 zijn aangewezen en aanbieders van vaste openbare telefoon-diensten of van openbare betaaltelefoons die langer dan tweeënvijftig weken dergelijke diensten leveren, maken jaarlijks voor 1 april op genoegzame wijze een overzicht over het voorafgaande kalenderjaar bekend van de kwaliteit van de door hen aangeboden diensten op basis van de in bijlage III van richtlijn nr. 2002/22/ EG gespecificeerde parameters, definities en meetmethoden. Het in de eerste volzin bedoelde overzicht bevat een beschrijving van de door de aanbieder genomen maatregelen om gelijkwaardige toegang voor eindgebruikers met een fysieke beperking te waarborgen. Het in de eerste volzin bedoelde overzicht wordt voor bekendmaking aan de Autoriteit Consument en Markt ter beschikking gesteld. Bij ministeriële regeling kunnen ten aanzien van de in het eerste lid genoemde verplichtingen nadere regels worden gesteld. Bij of krachtens algemene maatregel van bestuur kunnen, voor zover niet voorzien	Telecommunication Act, Article 7.4 Providers of public telephone services at a fixed location or of public pay telephones that have been designated pursuant to Article 9.2 and providers of fixed public telephone services that provide such services for more than 52 weeks shall publish an annual overview on 1 April of each year for the previous calendar year, in an adequate manner, regarding the quality of the services they provide on the basis of the parameters, definitions, and measurement methods specified in Annex III of Directive No. 2002/22/EC. The overview within the meaning of the first sentence shall include a description of the measures taken by the provider to guarantee equal access for end-users with a physical disability. The overview within the meaning of the first sentence shall be made available to the Board for publication. Specific rules may be set by ministerial order regarding the obligations within the meaning of paragraph 1. In so far as not provided pursuant to paragraph 1, specific rules may be set by or pursuant to a general administrative order regarding

op grond van het eerste lid, regels worden gesteld inzake het: door aanbieders van openbare elektronische communicatiediensten, aanbieders van openbare elektronische commu-nicatienetwerken of programmadiensten maken van een periodiek overzicht van de kwaliteit van de door hen aangeboden diensten aan de hand van bij of krachtens die algemene maatregel van bestuur te bepalen parameters, definities en meetmethoden; door de Autoriteit Consument en Markt, of een door de Autoriteit Consument en Markt aan te wijzen onafhankelijke deskundige derde, onderzoeken of het overzicht in overeenstemming is met de desbetreffende regels, en bekendmaken van het overzicht en het ter beschikking stellen daarvan aan de Autoriteit Consument en Markt. De regels, bedoeld in het derde lid, kunnen verschillen voor bij die regels te bepalen categorieën van openbare elektronische communicatie-diensten of programma-diensten. Bij de regels, bedoeld in het tweede en derde lid, kunnen taken worden opgedragen en bevoegdheden worden verleend aan de Autoriteit Consument en Markt.	the drawing up by providers of publicly available electronic communications services, providers of public electronic communications networks, or programme services of a periodic overview of the quality of the services they provide on the basis of para-meters, definitions, and measurement methods determined by means of a general administrative order; the investigation by the Board, or by an independent expert third party designated by the Board, of whether said overview is in accordance with the rules concerned; and the publication of said overview and its provision to the Board. The rules within the meaning of paragraph 3 may differ for certain categories of publicly available electronic communications services or programme services, as specified in said rules. The rules within the meaning of paragraphs 2 and 3 may assign tasks and powers to the Board
Telecommunicatiewet 1998 Artikel 7.4a(1): Bij of krachtens algemene maatregel van bestuur kunnen ter voorkoming van een achteruitgang van de dienstverlening en een belemmering of vertraging van het verkeer over openbare elektronische communicatienetwerken, nadere minimumvoorschriften inzake de kwaliteit van openbare elektronische communicatiediensten worden gesteld aan aanbieders van openbare elektronische communicatie-netwerken.	Dutch Telecommunication Act 1998 Article 7.4a(1) By or pursuant to an Order in Council, in order to prevent a decline in services and a hindrance or delay in traffic on public electronic communication networks, further minimum requirements regarding the quality of public electronic communication services may be imposed on providers of public electronic communication networks.
Telecommunicatiewet 1998 Artikel 11.7(1): Het gebruik van automatische oproep- en communicatiesystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor	Dutch Telecommunication Act 1998 Article 11.7(1): The use of automatic calling and communication systems without human intervention, faxes and electronic messages for the transmission of unsolicited communications for commercial, idealistic

commerciële, ideële of charitatieve doeleinden aan abonnees of gebruikers is uitsluitend toegestaan, mits de verzender kan aantonen dat de desbetreffende abonnee of gebruiker daarvoor voorafgaand toestemming heeft verleend, onverminderd hetgeen is bepaald in het tweede en derde lid.	or charitable purposes to subscribers or users is only permitted, provided that the sender can prove that the relevant subscriber or user has previously has granted permission, without prejudice to the provisions of paragraphs 2 and 3.
Uitvoeringswet Algemene Verordening gegevensbescherming (UAVG) 2018 Artikel 6: Er is een Autoriteit persoonsgegevens. De Autoriteit persoonsgegevens is de toezichthoudende autoriteit, bedoeld in artikel 51, eerste lid, van de verordening. Onverminderd artikel 57 van de verordening, heeft de Autoriteit persoonsgegevens tot taak toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de verordening of de wet bepaalde. Ter uitvoering van een bindende EU-rechtshandeling kunnen, gehoord de Autoriteit persoonsgegevens, bij regeling van Onze Minister aan de Autoriteit persoonsgegevens taken worden opgedragen.	Dutch GDPR Implementation Act 2018, Article 6: There is a Personal Data Authority. The Personal Data Authority is the supervisory authority, referred to in Article 51, first paragraph, of the Regulation. Without prejudice to Article 57 of the Regulation, the Authority has the task of supervising the processing of personal data in accordance with the provisions of and pursuant to the Regulation or the law. In order to implement a binding EU legal act, the Personal Data Authority may be assigned tasks by order of Our Minister to the Authority for personal data.
Uitvoeringswet Algemene Verordening gegevensbescherming (UAVG) 2018 Artikel 41: De verwerkingsverantwoordelijke kan de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34 van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van: de nationale veiligheid; landsverdediging; de openbare veiligheid; de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.	Dutch GDPR Implementation Act 2018, Article 41: The controller may not apply the obligations and rights referred to in Articles 12 to 21 and Article 34 of the Regulation to the extent that this is necessary and proportionate to guarantee: national security; national defence; public safety; the prevention, investigation, detection and prosecution of criminal offenses or the enforcement of penalties, including protection against and prevention of threats to public security.
Wet bescherming persoons-gegevens, Article 36 Degene aan wie overeen-komstig artikel 35 kennis is gegeven van hem betreffende persoonsgegevens, kan de verantwoordelijke verzoeken deze te verbeteren, aan te vullen,	Dutch Personal Data Protection Act, Article 36 A person who has been informed about personal data relating to him in accordance with Article 35 may request the responsible party to correct, supplement, delete or block

te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed. De verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. Indien de persoonsgegevens zijn vastgelegd op een gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, dan treft hij de voorzieningen die nodig zijn om de gebruiker van de gegevens te informeren over de onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming ondanks het feit dat er grond is voor aanpassing van de gegevens op grond van dit artikel. Het bepaalde in het eerste tot en met vierde lid is niet van toepassing op bij de wet ingestelde openbare registers, indien in die wet een bijzondere procedure voor de verbetering, aanvulling, verwijdering of afscherming van gegevens is opgenomen.	the said data in the event that it is factually inaccurate, incomplete or irrelevant to the purpose or purposes of the processing, or is being processed in any other way which infringes a legal provision. The request shall contain the modifications to be made. The responsible party shall inform the requester in writing within four weeks of receiving the request as to whether and, if so, to what extent, it is complying therewith. A refusal to do so must be accompanied by the reasons. The responsible party must make sure that a decision to correct, supplement, delete or block data is implemented as quickly as possible. Where personal data have been recorded on a data carrier to which no modifications can be made, the responsible party must take the necessary steps to inform the data user that it is impossible to correct, supplement, delete or block the data, even where there are grounds under this article for modifying the data. The provisions of (1) to (4) do not apply to public registers set up by law where this law provides for a special procedure for correcting, supplementing, deleting or blocking data.
Wet op de Inlichtingen- en veiligheidsdiensten (Wiv) 2017, Artikel 6: Onze betrokken Ministers gezamenlijk stellen de geïntegreerde aanwijzing voor de uitvoering van de in artikel 8, tweede lid, onder a en d, onderscheidenlijk artikel 10, tweede lid, onder a, c en e bedoelde taken vast. De geïntegreerde aanwijzing heeft een looptijd van vier jaren. Onze betrokken Ministers bezien jaarlijks aan de hand van voorstellen van de commissie als bedoeld in artikel 5 of de geïntegreerde aanwijzing aanpassing behoeft. De vaststelling van de geïntegreerde aanwijzing alsmede daarop aan te brengen aanpassingen geschiedt niet dan nadat ter zake overleg is gevoerd met Onze Ministers	Intelligence Secret Services Act 2017, Article 6: Our relevant Ministers jointly adopt the integrated instruction for the performance of the duties referred to in Article 8, second paragraph, under a and d, and Article 10, second paragraph, under a, c and e. The integrated designation has a duration of four years. Our relevant Ministers examine annually on the basis of proposals from the committee as referred to in Article 5 whether the integrated designation requires adjustment. The adoption of the integrated designation and the adjustments to be made thereto shall only take place after consultation has been held with Our Ministers of Foreign Affairs and of Security and Justice.

van Buitenlandse Zaken en van Veiligheid en Justitie.	
Wet op de Inlichtingen- en veiligheidsdiensten (Wiv) 2017, Artikel 24: De hoofden van de diensten dragen er voorts zorg voor dat de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens deze wet is bepaald. Tot de maatregelen, bedoeld in het eerste lid, behoren in ieder geval: de nodige voorzieningen ter bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt alsmede ter bevordering van de kwaliteit van de gegevensverwerking, waaronder begrepen de daarbij gehanteerde algoritmen en modellen; de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens alsmede tegen onbevoegde gegevensverwerking; de aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn tot de bij de aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens.	Intelligence Secret Services Act 2017, Article 24: The heads of services also ensure that the technical, human and organisational measures related to the processing of data are in accordance with the provisions of or pursuant to this Act. The measures meant in the first paragraph include in any case: the necessary provisions to promote the correctness and completeness of the data being processed and to promote the quality of data processing, including the algorithms and models used for this; the necessary provisions of a technical and organisational nature to protect data processing against loss or corruption of data as well as against unauthorized data processing; the designation of persons who, to the exclusion of others, are authorised to perform the work specified in the designation within the framework of data processing.
Wetboek van Strafrecht, Article 54 Bij misdrijven door middel van de drukpers gepleegd wordt de drukker als zodanig niet vervolgd, indien het gedrukte stuk zijn naam en woonplaats vermeldt en de persoon op wiens last het stuk is gedrukt, bekend is of op de eerste aanmaning van de rechter-commissaris, door de drukker is bekendgemaakt. Deze bepaling is niet toepasselijk, indien de persoon op wiens last het stuk is gedrukt, op het tijdstip van het drukken strafrechtelijk niet vervolgbaar of buiten het Rijk in Europa gevestigd was.	Dutch Criminal Code, Article 54 In the case of serious offences committed by means of a printing press, the printer shall not be 44 prosecuted in his capacity as printer if his name and address appear on the printed matter and if the identity of the offender is known or if, upon first notice, after institution of a preliminary inquiry, the printer has disclosed the identity of the offender. This provision shall not apply if the natural or legal person, who/which commissioned the printing of the item, could not be prosecuted or was resident or established outside the Kingdom in Europe.
Wetboek van Strafrecht, Article 54a Een tussenpersoon die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt bij een strafbaar feit dat met gebruikmaking van die	Dutch Criminal Code, Article 54a An intermediary which provides a telecommunication service that consists of the transfer or storage of data from a third party, shall not be prosecuted in its capacity as intermediary telecommunication provider

dienst wordt begaan als zodanig niet vervolgd indien hij voldoet aan een bevel als bedoeld in artikel 125p van het Wetboek van Strafvordering.	if it complies with an order as described in article 125p of the Dutch Code of Criminal Procedures.
Wetboek van Strafrecht, Artikel 111: vervallen per 1.1.2020	Dutch Criminal Code, Article 111: repealed by 1.1.2020
Wetboek van Strafrecht, Artikel 114(2): vervallen per 1.1.2020	Dutch Criminal Code, Article 114(2): repealed by 1.1.2020
Wetboek van Strafrecht, Artikel 118: vervallen per 1.1.2020	Dutch Criminal Code, Article 118: repealed by 1.1.2020
Wetboek van Strafrecht, Artikel 131: Hij die in het openbaar, mondeling of bij geschrift of afbeelding, tot enig strafbaar feit of tot gewelddadig optreden tegen het openbaar gezag opruit, wordt gestraft met gevangenisstraf van ten hoogste vijf jaren of geldboete van de vierde categorie. Indien het strafbare feit waartoe wordt opgeruid een terroristisch misdrijf dan wel een misdrijf ter voorbereiding of vergemakkelijking van een terroristisch misdrijf inhoudt, wordt de gevangenisstraf, gesteld op het in het eerste lid omschreven feit, met een derde verhoogd.	Dutch Criminal Code, Article 131 He who in public, verbal or written or portrayed, for any offense or for violent action against the public authority, is punished with imprisonment of at most five years or a fine of the fourth category. If the offense to which the offense refers is a terrorist crime or a crime to prepare for or facilitate a terrorist crime, the prison sentence based on the fact described in the first paragraph is increased by a third.
Wetboek van Strafrecht, Article 137c Hij die zich in het openbaar, mondeling of bij geschrift of afbeelding, opzettelijk beledigend uitlaat over een groep mensen wegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuele gerichtheid of hun lichamelijke, psychische of verstandelijke handicap, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.	Dutch Criminal Code, Article 137c Anyone who publicly, orally, in writing or graphically, intentionally expresses himself insultingly regarding a group of people because of their race, their religion or their life philosophy, their heterosexual or homosexual orientation or their physical, psychological or mental disability, shall be punished by imprisonment of no more than a year or a monetary penalty of the third category
Wetboek van Strafrecht, Article 137d Hij die in het openbaar, mondeling of bij geschrift of afbeelding, aanzet tot haat tegen of discriminatie van mensen of gewelddadig optreden tegen persoon of goed van mensen wegens hun ras, hun godsdienst of levensovertuiging, hun geslacht, hun hetero- of homoseksuele gerichtheid of hun lichamelijke, psychische of verstandelijke handicap, wordt gestraft met gevangenisstraf	Dutch Criminal Code, Article 137d Anyone who publicly, orally or in writing or image, incites hatred or discrimination against persons or violence against person or property on the grounds of their race, religion or beliefs, their gender, their heterosexual or homosexual orientation or their physical, psychological or mental, shall be punished with imprisonment not exceeding one year or fine of the third category.

van ten hoogste twee jaren of geldboete van de vierde categorie.	
Wetboek van Strafrecht, Artikel 240: Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die een afbeelding, een voorwerp of een gegevensdrager, bevattende een afbeelding waarvan de vertoning schadelijk is te achten voor personen beneden de leeftijd van zestien jaar, verstrekt, aanbiedt of vertoont aan een minderjarige van wie hij weet of redelijkerwijs moet vermoeden, dat deze jonger is dan zestien jaar.	Dutch Criminal Code, Article 240: A prison sentence of no more than one year or a fine of the fourth category is punishable by those who provide, present or display an image, an object or a data carrier, containing an image whose display is considered harmful to persons under the age of sixteen. to a minor whom he knows or should reasonably suspect is under the age of sixteen.
Wetboek van Strafrecht, Article 240b Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie wordt gestraft degene die een afbeelding - of een gegevensdrager, bevattende een afbeelding - van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken, verspreidt, aanbiedt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert, verwerft, in bezit heeft of zich door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst de toegang daartoe verschaft. Met gevangenisstraf van ten hoogste acht jaren of geldboete van de vijfde categorie wordt gestraft degene die van het plegen van een van de misdrijven, omschreven in het eerste lid, een beroep of een gewoonte maakt.	Dutch Criminal Code, art 240b Any person who distributes, offers, publicly displays, produces, imports, conveys in transit, exports, obtains, possesses or accesses by means of a computerised device or system or by use of a communication service an image - or a data carrier that contains an image - of a sexual act involving or seemingly involving a person who is manifestly under the age of eighteen years, shall be liable to a term of imprisonment not exceeding four years or a fine of the fifth category. Any person who makes a profession or habit of committing any of the serious offences defined in subsection (1), shall be liable to a term of imprisonment not exceeding eight years or a fine of the fifth category.
Wetboek van Strafrecht, Artikel 261: Hij die opzettelijk iemands eer of goede naam aanrandt, door telastlegging van een bepaald feit, met het kennelijke doel om daaraan ruchtbaarheid te geven, wordt, als schuldig aan smaad, gestraft met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie. Indien dit geschiedt door middel van geschriften of afbeeldingen, verspreid, openlijk tentoongesteld of aangeslagen, of door geschriften waarvan de inhoud openlijk ten gehore wordt gebracht, wordt	Dutch Criminal Code, Article 261: He who deliberately assassinates someone's honour or good name by blaming a certain fact for the apparent purpose of publicising it is punished, as guilty of defamation, with imprisonment of up to six months or a fine of the third category. If this is done by means of writings or images, distributed, openly exhibited or excited, or by writings whose contents are publicly heard, the perpetrator, as guilty of defamation, is punished with imprisonment of up to one year or a fine of up to one year. the third category.

de dader, als schuldig aan smaadschrift, gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.	
Wetboek van Strafrecht, Article 262: Hij die het misdrijf van smaad of smaadschrift pleegt, wetende dat het te last gelegde feit in strijd met de waarheid is, wordt, als schuldig aan laster, gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie. Ontzetting van de in artikel 28, eerste lid, onder 1° en 2°, vermelde rechten kan worden uitgesproken.	Dutch Criminal Code, Article 262: He who commits the crime of defamation or defamation, knowing that the offense is contrary to the truth, is, as guilty of defamation, punished with imprisonment of up to two years or a fine of the fourth category. Removal of the rights referred to in Article 28, first paragraph, under 1 ° and 2 °, can be pronounced.
Wetboek van Strafrecht, Article 267 De in de voorgaande artikelen van deze titel bepaalde gevangenisstraffen kunnen met een derde worden verhoogd, indien de belediging wordt aangedaan aan: het openbaar gezag, een openbaar lichaam of een openbare instelling; een ambtenaar gedurende of ter zake van de rechtmatige uitoefening van zijn bediening; het hoofd of een lid van de regering van een bevriende staat.	Dutch Criminal Code, Article 267 The terms of imprisonment prescribed in the preceding sections of this Part may be increased by one third, if the defamation is made in regard of: the public authorities, a public body or a public institution; a civil servant during or in connection with the lawful performance of his office; the head or a member of the government of a friendly nation.
Wetboek van Strafrecht, Artikel 268: Hij die opzettelijk tegen een bepaald persoon bij de overheid een valse klacht of aangifte schriftelijk inlevert of in schrift doet brengen, waardoor de eer of goede naam van die persoon wordt aangerand, wordt, als schuldig aan lasterlijke aanklacht, gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie. Ontzetting van de in artikel 28, eerste lid, onder 1° en 2°, vermelde rechten kan worden uitgesproken.	Dutch Criminal Code, Article 268: He who deliberately submits a false complaint or report to the government against a certain person in writing or has it brought into writing, whereby the honour or good name of that person is assaulted, is, as guilty of defamatory indictment, punished with imprisonment of at most two years or a fine of the fourth category. Removal of the rights referred to in Article 28, first paragraph, under 1 ° and 2 °, can be pronounced.
Wetboek van Strafrecht, Article 271 Hij die een geschrift of afbeelding van beledigende of voor een overledene smadelijke inhoud verspreidt, openlijk tentoonstelt of aanslaat of, om verspreid, openlijk tentoongesteld of aangeslagen te worden, in voorraad heeft, wordt, indien hij weet of ernstige reden heeft om te vermoeden dat de inhoud van het geschrift of de afbeelding van zodanige aard is, gestraft met gevangenisstraf van ten hoogste	Dutch Criminal Code, Article 271 Any person who distributes, publicly displays or posts, or has in store to be distributed, publicly displayed or posted, written matter or an image whose contents are insulting or, with regard to a deceased person, slanderous or libellous, if he knows or has serious reason to suspect that the written matter or the image contains such, shall be liable to a term of imprisonment not exceeding three months or a fine of the second category.

drie maanden of geldboete van de tweede categorie. Met dezelfde straf wordt gestraft hij die, met gelijke wetenschap of een gelijke reden tot vermoeden, de inhoud van een zodanig geschrift openlijk ten gehore brengt. Indien de schuldige een van de misdrijven omschreven in dit artikel in zijn beroep begaat en er tijdens het plegen van het misdrijf nog geen twee jaren zijn verlopen sedert een vroegere veroordeling van de schuldige wegens een van deze misdrijven onherroepelijk is geworden, kan hij van de uitoefening van dat beroep worden ontzet. De misdrijven worden niet vervolgd dan op klacht van de in artikel 269 en het tweede lid van artikel 270 aangewezen personen, behalve in de gevallen voorzien in artikel 267.	Any person who, with the same knowledge or reason to suspect such, publicly utters the contents of such written matter shall be liable to the same punishment. If the offender commits any of the serious offences defined in this section in the practice of his profession and if at the time of commission of the serious offence two years have not yet expired since a previous conviction of the offender for any of these serious offences became final, he may be disqualified from the practice of that profession. The serious offences shall be prosecuted only on complaint of the persons designated in Article 269 and Article 270(2), except for the cases provided for in the opening lines of section 267.
Wetboek van Strafvordering, Article 126zi 1. In geval van aanwijzingen van een terroristisch misdrijf kan de opsporingsambtenaar in het belang van het onderzoek een vordering doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst in de zin van artikel 138h. Artikel 126n, tweede lid, is van toepassing. 2. Indien de gegevens, bedoeld in het eerste lid, bij de aanbieder niet bekend zijn en zij nodig zijn voor de toepassing van artikel 126zf of artikel 126zg kan de officier van justitie in het belang van het onderzoek vorderen dat de aanbieder de gevorderde gegevens op bij algemene maatregel van bestuur te bepalen wijze achterhaalt en verstrekt. 3. Artikel 126na, derde en vierde lid, is van overeenkomstige toepassing.	Dutch Code of Criminal Procedures, Article 126zi 1. In the case of indications of a terrorist offence, the investigating officer may, in the interest of the investigation, request the provision of data pertaining to name, address, postal code, town, number and type of service of a user of a communication service within the meaning of article 126la. Article 126n(2) shall apply. 2. If the data, referred to in subsection (1), is not known to the provider and is necessary for the application of section 126zf or section 126zg, the public prosecutor may, in the interest of the investigation, request the provider to retrieve and provide the requested data in a manner to be determined by Governmental Decree. 3. Section 126na (3) and (4) shall apply mutatis mutandis.

Bibliography

English titles

Legislation

Appendix to Recommendation CM/Rec (2016)5 of the Committee of Ministers to member States on Internet freedom

Charter of the Fundamental Rights of the European Union [2007] OJ C 303/17

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

Council of Europe, Convention on Cybercrime (Budapest 2001)

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178

Directive 2000/31/EC of the European Parliament of 8 June 2000 in certain Legal aspects of information society services, in particular electronic commerce in the Internal Market, O.J. 2000, L178.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [1995] OJ L 281 /1

Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM/2016/0593 final - 2016/0280 (COD)

European Convention on Human Rights (as amended by Protocols Nos. 11 and 14)

European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD))

Human Right Committee Resolution A/HRC/38/L.10/Rev.1 on the The promotion, protection and enjoyment of human rights on the Internet

General Policy Recommendation No. 15 of the European Commission against Racism and Intolerance (ECRI) on national legislation to combat racism and racial discrimination, 8 December 2015

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

Recommendation No. R 97(20) of the Committee of Ministers of the Council of Europe to Member States on 'hate speech', 30 October 1997

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *OJ L 119, 4.5.201*

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

UN Human Rights Committee (HRC), CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988)

UN Human Rights Committee, General comment No 34 102nd session (12 September 2011)

UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, UN Doc. A/RES/45/95 (14 December 1990)

The Universal Declaration of Human Rights (UDHR) of 10 December 1948

Reports

Benedek W and Kettemann M, 'Freedom of Expression and the Internet' (2013) Council of Europe Publishing

Clark J et al, 'The Shifting Landscape of Global Internet Censorship.' (2017) Berkman Klein Center for Internet & Society Research Publication

Council of Europe and the Swiss Institute of Comparative Law, Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content [2017].

Council of Europe: European Court of Human Rights, *Fact sheet - Hate Speech*, February 2020 < https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf>

ECRI (2019), Fifth Report on the Netherlands CRI(2019)19 < https://rm.coe.int/fifth-report-on-the-netherlands/168094c577> last accessed 18 January 2020.

'Freedom Of The Press 2017: Netherlands' (Freedom House 2017) <https://freedomhouse.org/report/freedom-press/2017/netherlands> last accessed 18 January 2020

International Telecommunication Union (ITU), Core House Indicators Rep 2019, < https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/CoreHouseholdIndicators.xlsx > accessed 13 February 2020

Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative 494

Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative

Memo on Code of Conduct on countering illegal online hate speech 2nd monitoring, 1 June 2017, IP/17/1471

Ministry of Foreign Affairs (2018), "International human rights policy: activities and results" Human Rights Report 2018

Mujic Z, Yazici D, and Stone M, 'Freedom of Expression on the Internet' (2012) OSCE, 266.

Quintais J, 'Global Online Privacy Study: Legal Background Report ' (2018) University of Amsterdam, Faculty of Law, Institute for Information Law

The Council of Europe, 'Comparative Study on Blocking, Filtering And Take-Down of Illegal Internet Content' (Lausanne, 2015)

Books

Adrian Shahbaz, "*The Rise of Digital Authoritarianism*", Freedom of the Net 2018 (2018)

Cohen-Almagor R, Confronting the Internet's dark side: moral and social responsibility on the free highway (Cambridge University Press 2015)

Council of Europe, *Comparative study on blocking, filtering and take-down of illegal internet content* (Council of Europe 2017)

Habermas J, Technology and Science as ideology (1st, Beacon Press 1971)

Koltay A, New Media and Freedom of Expression: Rethinking the Constitutional Foundations of the Public Sphere (Hart Publishing 2019)

Koops B and Groothuis M, 'Constitutional Rights and Technology in the Netherlands' in Leendes R, Goops B, and De Her P (eds.) *Constitutional Rights and New Technologies* (Asser Press, 2008)

Nijman JE et Werner WG, Netherlands Yearbook of International Law 2018: Populism and International Law (Springer Nature 2019) 283

Nowak M. (2003) 'An Introduction to International Human Rights Regime', Nijhoff.

Romano, A. (2009). Public Sentinel: News Media and Governance Reform. (P. Norris, Ed.) World Bank Publications.

Tsagourias N et Buchan R, Research Handbook on International Law and Cyberspace (Edward Elgar Publishing, 2015)
<https://books.google.nl/books?id=9ufECQAAQBAJ&lpg=PA225&ots=ypiseX3eIZ&dq=cable%20bound%20communications&hl=it&pg=PA218#v=onepage&q=cable%20bound%20communications&f=false > accessed 16 February 2020

Wimmer, R., & Dominick, J. (2011). Mass media research: An introduction (9th ed.). Belmont, CA: Thompson Wadsworth.

Periodicals

A.J. Verheij, *'The right to be forgotten – a Dutch perspective'* (2016) International Review of Law, Computers & Technology, 30:1-2, 32-41, DOI: 10.1080/13600869.2015.1125156

Eskens S, Helberger N, Moeller J, 'Challenged by news personalisation: five perspectives on the right to receive information' [2017] 9(2) Journal of Media Law 25

Haim M, Graefe A, and Brosius H, 'Burst of the Filter Bubble?' [2017] 6(3) Digital Journalism 330

Ho Youm K & Park A, *'The "Right to Be Forgotten" in European Union Law: Data Protection Balanced With Free Speech?'* (2016) Journalism & Mass Communication Quarterly, Vol. 93(2) 273

Holger Bleich, (2018). "EU demands online platform upload filter immediately", Heise.

Joost Schellevis, "Politics says no to internet filter" Tweakers, 18 May 2011

Koops B.-J., 'Cybercrime Legislation in the Netherlands' [2010] Electronic Journal of Comparative Law, vol 14.3

Kulk S & Borgesiu Z K, '*Freedom of Expression and 'Right to Be Forgotten' Cases in the Netherlands After Google Spain'* (2015) EDPL Freedom of Expression and 'Right to Be Forgotten', volume 1, issue 2, 113

Lodder A and Sandvliet K, 'Comparative study on blocking filtering and take-down of illegal internet content - Netherlands' (2015) The Council of Europe and Swiss Institute of Comparative Law Comparative

Matthias Monroy, "Facebook, Twitter & Co: Upload-Filter gegen 'Terrorismus und Extremismus' gestartet" [Facebook, Twitter, and co.: upload filter against 'terrorism and extremism' activated], Netzpolitik.org, March 13, 2017

Rene Schoemaker, WebWereld (IDG Netherlands), 7 March 2011

Rosen J, 'The Right to Be Forgotten' (2012) 64(88) Stanford Law Review Online 88-92

Soma J and Norman N, 'International Take-Down Policy: A Proposal for WTO and WIPO to Establish International Copyright Procedural Guidelines for Internet Service Providers', (2000) 22(391) Hastings Communications and Entertainment Law Journal

Stol W, Kaspersen H, and others, 'Government filtering of websites: The Dutch Case' [2009] 25(3) *Computer Law &Security Review* 251

Digital resources

'About - NUJ Netherlands' (*Nuj-netherlands.nl*) <https://nuj-netherlands.nl/about-nuj-netherlands> accessed 9 February 2020

'Coalition Of Countries For Free Internet' (Government.nl, 2011) <https://www.government.nl/latest/news/2011/12/14/coalition-of-countries-for-free-internet> accessed 18 January 2020

'History - Freedom Online Coalition' (*Freedom Online Coalition*) <https://freedomonlinecoalition.com/about-us/history/> accessed 25 January 2020

'Human Rights In The Netherlands' (Government.nl) <https://www.government.nl/topics/human-rights/human-rights-in-the-netherlands> accessed 18 January 2020

'Limits on Freedom of Expression: Netherlands' (*Library of Congress, 2019)* < https://www.loc.gov/law/help/freedom-expression/netherlands.php#_ftnref6>

'Over MiND' (Meldpunt Internet Discriminatie (MiND), 2013), < https://www.mindnederland.nl/> accessed 10 February 2020.

'Tolerance and Non-Discrimination Department' (*OSCE Office for Democratic Institutions and Human Rights (ODIHR)*, 2018) < https://hatecrime.osce.org/netherlands> accessed 7 February 2020

Barlow JP, A Declaration of the Independence of Cyberspace, (1996), < https://www.eff.org/cyberspace-independence > accessed 11 February 2020

Beauchere J, 'Revenge Porn: Putting Victims Back in Control' (*Microsoft Blog,* 22 July 2015) <https://blogs.microsoft.com/on-the-issues/2015/07/22/revenge-porn-putting-victims-back-in-control/> last accessed 3 February 2020

Burke J, 'The Murder That Shattered Holland's Liberal Dream' (*the Guardian*, 2004) <https://www.theguardian.com/world/2004/nov/07/terrorism.religion> accessed 2 February 2020

Carlijn Dohmen, 'Notice and Take Down: Towards a central system in the Netherlands' < http://arno.uvt.nl/show.cgi?fid=81096> last accessed 14 February 2020

Céline van Waesberge, 'Dutch surgeon successfully invokes the right to be forgotten' (Loyens&Loef 4 March 2019)

Cohen JE, 'Law for the Platform Economy' (2017) 191, 51 U.C. Davis L Rev 133-204 < https://lawreview.law.ucdavis.edu/issues/51/1/symposium/51-1_Cohen.pdf > accessed 11 February 2020

Council of Europe, Guide on Article 8 of the Convention - Right to respect for private and family life (updated 31 August 2019) 37
<https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf >
accessed 17 February 2020

European Data Protection Board (EDPB 2018), Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, available at
< https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf > accessed 15 February 2020

Expat-news/netherlands-ranks-first-globally-press-freedom>
accessed 5 February 2020

Freedomhouse, Netherlands Freedom Rep 2019
< https://freedomhouse.org/report/freedom-world/2019/netherlands >
accessed 16 February 2020

Gerechtshof Amsterdam 19 augustus 2014 (NSE), ECLI:NL:GHAMS:2014:3435 (*Internetrechtspraak,* 16 February 2020) <https://internetrechtspraak.com/gerechtshof-amsterdam-19-augustus-2014-nse-eclinlghams20143435/>
last accessed 16 February 2020

Gowling A, 'The Netherlands ranks first globally for press freedom' (*I am Expat* 8 March 2014) <https://www.iamexpat.nl/expat-info/dutch-

Incriminating Joke caviar texts, available at <https://13-september.nl/inciting-texts/ >
accessed 17 February 2020

IViR, 'Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?' (Utrecht/Amsterdam, March 2018), < https://www.ivir.nl/publicaties/download/Wiv_2017.pdf > accessed 16 February 2020

JOINT DECLARATION by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression (2002)27
< https://www.osce.org/fom/99558?download=true > accessed 17 February 2020

Kang J, "Information Privacy in Cyberspace Transactions" (1998) Stanford LR 50 1202–1205

Kingdom of the Netherlands, 'Factsheet on the judiciary in the Netherlands' (*The Netherlands and You*, 21 September 2019) <https://www.netherlandsandyou.nl/latest-news/news/2017/09/21/factsheet-on-the-judiciary-in-the-netherlands> last accessed 7 February 2020

Leiden University, The Netherlands One of the Leaders in Privacy Protection, (2017) <https://perma.cc/QH4Z-TKH3.> accessed 16 February 2020

Martinez S, 'Dutch King: Should Insulting Him Be A Crime?' (mlive, 2019) <https://www.mlive.com/business/west-michigan/2015/05/dutch_king_should_insulting_hi.html> accessed 18 January 2020

OSCE, Defamation and Insult Laws in the OSCE Region: A Comparative Study (2017) 7 < https://www.osce.org/fom/303181?download=true > accessed 17 February 2020

Phoa P, 'Country report the netherlands case study (ii) on freedom of expression in the context of the media' (Beucitizens 2016) <https://webcache.googleusercontent.com/search?q=cache:B64gb3NK5qUJ:https://www.uu.nl/en/files/case-study-ii-on-freedom-of-expression-in-the-context-of-the-media-d7-4pdf+&cd=2&hl=it&ct=clnk&gl=nl&client=safari> accessed 17 February 2020

phys.org, 'France and Netherlands plan Internet anti-censorship drive' (*phys.org* 25 May 2010) <https://phys.org/news/2010-05-france-netherlands-internet-anti-censorship.html> accessed 7 February 2020

Schuetze C, 'Dutch Parliament Reduces Penalties For Insulting King' (The Sydney Morning Herald, 2018) <https://www.smh.com.au/world/europe/dutch-parliament-reduces-penalties-for-insulting-king-20180411-p4z8yx.html> accessed 18 January 2020

Secretary-General of the European Commission, 'Commission Staff Working Document Impact Assessment: Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online' (2018) SWD (2018)409 final, 131 <https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkrs7l664lz7> last accessed 13 February 2020

Stam J, 'The Risky Aspects Of Our Hate Speech Laws' (*Leidenlawblog.nl*, 2019) <https://leidenlawblog.nl/articles/the-risky-aspects-of-our-hate-speech-laws> accessed 23 January 2020

Summary of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law, 15 June 2014 < Summary of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law, 15 June 2014 <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:l33178> accessed 25 February 2020.

TBO, 'Dutch Supreme Court remands Pirate Bay Case for Review' (*Trademarks and Brands Online,* 4 July 2018)
<https://www.trademarksandbrandsonline.com/news/dutch-supreme-court-remands-pirate-bay-case-for-review-5265> last accessed 16 February 2020

The Freedom Online Coalition
<https://freedomonlinecoalition.com/about-us/history/>
last accessed 15 February 2020

Van Der Putt Pet al, 'Data Protection & Cybersecurity 2019' (Chambers and Partners, 8 May 2019) < https://practiceguides.chambers.com/practice-guides/data-protection-cybersecurity-2019/netherlands > accessed 16 February 2020

Van Eijk N, 'Does net neutrality work? The Dutch case' (27th European Regional Conference of the International Telecommunications Society 2016)
<https://www.econstor.eu/bitstream/10419/148715/1/van-Eijk.pdf >
accessed 14 February 2020

Van Eijk N, "Net Neutrality in the Netherlands" (2014) 7(1) J of Law and Economic Regulation < https://hdl.handle.net/11245/1.445987 > accessed 14 February 2020

Case law

Ahmet Yildirim v. Turkey App no 3111/10 (ECtHR, 18 December 2012), para 54, <http://hudoc.echr.coe.int/eng?i=001-115705>

Ashby Donald and others v. France app no 36769/08 (ECHR,10 January 2013)

Axel Springer AG v. Germany app 39954/08 (ECHR [GC], 7 February 2012)

C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited (CJEU, 3 October 2019)

Case C-131/12 *Google Spain and Google* EU:C:2014: 317, [2014] ECR

Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2014] ECLI:EU:C:2014:317

Case C-610/15 CJEU Judgement Stichting Brein v Ziggo BV and XS4All Internet BV (2017) ECLI:EU:C:2017:456

Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH [2019]

Chauvy and Others v. France app no 64915/01 (ECHR 29 September 2004)

Delfi AS v. Estonia App no 64569/09 (ECtHR, 10 October 2013)

Handyside v. United Kingdom app no 5493/72 (ECHR, 7 December 1976)

Handyside v. the United Kingdom App No.5493/72, (ECtHR, 7 Decemeber 1976), <http://hudoc.echr.coe.int/eng?i=001-57499>

Leroy v. France app no 36109/03 (ECHR, 2 October 2008)

Lingens v. Austria app no 9815/82 (ECHR, 8 July 1986)

Mouvement Raëlien v. Switzerland app no 16354/06 (ECHR [GC], 13 July 2012)

Neij and Sunde Kolmisoppi v. Sweden app no 40397/12 (ECHR, 19 February 2013 "The Pirate Bay")

Sanoma Uitgevers B.V. v The Netherlands app no 38224/03 (ECHR, 14 September 2010)

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland app no 931/13 (ECHR 27 June 2017)

Söderman v. Sweden app no 5786/08 (ECHR, 12 November 2013)

Springer v. Germany app no 39954/08 (ECHR, 7 February 2012)

Sunday Times v United Kingdom app no 6538/74 (ECHR, 26 April 1979)

Tamiz v. the United Kingdom app no 3877/14 (ECHR 19 September 2017)

Telegraaf and Others v. the Netherlands app no 39315/06 (ECHR, 22 November 2012)

Times Newspapers Ltd (Nos. 1 and 2) v. the United Kingdom app nos s. 23676/03 and 3002/03 (ECHR 2009)

Von Hannover v. Germany (n 2), app nos 40660/08 and 60641/08 (ECHR, 7 February 2012)

Yildirim v. Turkeyapp no 3111/10 (ECHR, 18 December 2012)

Dutch titles

Legislation

Act on the re-use of public information [Wet Hergebruik Overheidsinformatie van 18 juli 2015 (WHO)]

Act on the Registration of Personal Data [Wet bescherming persoonsgegevens van 25 mei 2018]

Constitution of the Kingdom of the Netherlands [Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815]

Copyright Act [Auteurswet van 23 september 1912]

Dutch Civil Code [Nederlands Burgerlijk Wetboek van 1 januari 1992]

Dutch Code of Criminal Procedures [Wetboek van Strafvordering van 16 januari 1912]

Dutch Criminal Code [Nederlands Wetboek van Strafrecht van 3 maart 1881]

Dutch Implementation Act [Uitvoeringswet AVG van 16 mei 2018]

Freedom of Information Act [Wet openbaarheid van bestuur van 10 maart 2010 (WOB)]

Intelligence and security services Act [Wet op de Inlichtingen- en veiligheidsdiensten van 26 juli 2017]

Media Act [Mediawet van 29 december 2008]

Notice and takedown Code of Conduct [Notice and takedown Gedragscode van 13 december 2018]

Telecommunication Act [Telecommunicatiewet van 19 oktober 1998]

Reports

Handleiding Wet Hergebruik Van Overheidsinformatie (Ministerie van Binnenlandse zaken en Koninkrijksrelaties 2015)
<https://open-overheid.nl/wp-content/uploads/2016/01/WEB_88737_handleiding_A5.pdf>
accessed 2 February 2020

Books

Bunschoten, D.E. 'Artikel 7' in J.H. Nieuwenhuis, C.J.J.M. Stolker, mr. W.L. Valk (eds) *Grondwet en Statuut Tekst & Commentaar* (5th ed, Wolters Kluwer 2018)

Van der Linden-Smith M. and Lodder A.R., Jurisprudentie Internetrecht 2009-2015 (Deventer: Kluwer 2015) [Dutch].

Periodicals

Kulk S, 'De Aansprakelijkheid van Platforms voor Auteursrechtinbreuken' [2007] Utrecht University [Dutch].

Digital resources

Autoriteit Consument & Markt, 'Netneutraliteit' <https://www.acm.nl/nl/onderwerpen-telecommunicatie-internet/netneutraliteit> accessed 15 February 2020 [Dutch].

Autoriteit Persoonsgegevens, Focus AP 2020-2023, available in Dutch at < https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf > accessed 15 February 2020

Jan-Jaap Oerlemans, 'Filtering the Internet for Law enforcement purposes?' <https://leidenlawblog.nl/articles/filtering-the-internet-for-law-enforcement-purposes> last accessed 15 February 2020

Kamerbrief over de Wet op de Inlichtingen- en veiligheidsdiensten, available in Dutch at <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/04/25/kamerbrief-over-de-wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv/kamerbrief-over-de-wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv.pdf. > accessed 16 February 2020; see also in Dutch <https://www.parool.nl/nieuws/invoering-sleepwet-uitgesteld-tot-1-mei~b655ba4f/ > accessed 16 February 2020

'Taakstraf Voor Beledigen Koningin Maxima' (*Rechtspraak.nl*, 2020) <https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Midden-Nederland/Nieuws/Paginas/Taakstraf-voor-beledigen-koningin-Maxima.aspx?pk_campaign=rssfeed&pk_medium=rssfeed&> accessed 18 January 2020

Case law

AI5638 [2003] Court of Appeal 's-Gravenhage NJ [2003]

AR2018/45 [2018] Court of Overijssel [2018]

AT2056 [2005] Dutch Supreme Court NJ 9 [2006]

AU4019 [2005] Dutch Supreme Court NJ 550 [2009]

BD1146 [2008] Court of Haarlem LJN [2008]

BK 1067 [2009] Court of Amsterdam [2009]

ECLI:NL:GHAMS:2014:3435, 19 August 2014

ECLI:NL:GHARN:2005:AT0895, Arnhem Court of Appeal

ECLI:NL:RBALM:2012:BY1807, District Court of Almelo

ECLI:NL:RBAMS:2014:1680, District Court of Amsterdam

ECLI:NL:RBAMS:2015:3984, District Court of Amsterdam

ECLI:NL:RBAMS:2017:3349

ECLI:NL:RBNHO:2013:BY9120, District Court of Harleem

ECLI:NL:RBROT:2009:BI1786, District Court of Rotterdam

ECLI:NL:RBSGR:2007:AZ5678, Court of The Hague

ECLI:NL:RBSGR:2007:BB8427, District Court of The Hague

Gerechtshof Amsterdam 15 februari 2018, ECLI:NL:GHAMS:2018:536, ECLI:NL:GHAMS:2018:537 en ECLI:NL:GHAMS:2018:538

Gerechtshof Amsterdam, 31 March 2015, ECLI:NL:GHAMS:2015:1123

RBSGR (Rechtbank 's-Gravenhage) 09-12-2016 ECLI:NL:RBDHA:2016:15014 [online].

RBSGR (Rechtbank 's-Gravenhage) 10-05-2012, ECLI:NL:RBSGR:2012:BW5387 [online]

Rechtbank Amsterdam 18 mei 2017, ECLI:NL:RBAMS:2017:3352, ECLI:NL: RBAMS:2017:3343, ECLI:NL:RBAMS:2017:3344, ECLI:NL:RBAMS:2017:3346, ECLI:NL:RBAMS:2017:3347, ECLI:NL:RBAMS:2017:3349

Rechtbank Amsterdam, 13 February 2015, ECLI:NL:RBAMS:2015:716

Rechtbank Amsterdam, 18 September 2014, ECLI:NL:RBAMS:2014:6118

Rechtbank Amsterdam, 23 juni 2011, ECLI:NL:RBAMS:2011:BQ9001

Rechtbank Den Haag, 9 december 2016, ECLI:NL:RBDHA:2016:15014

Supreme Court of the Netherlands ECLI: NL: HR: 2018: 1046 <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:PHR:2018:202>

ELSA North Macedonia

Contributors

National Academic Coordinator

Angela Angjelovska

National Researchers

Kristina Petrova

Ivana Baltovska

Elena Atanasoska

Marko Paloski

Blagoj Milev

Nikola Murdzev

Beba Zhagar

Simona Pecalevska

National Linguistic Editor

Marta Minchevska

National Technical Editor

Bojana Rusevska

National Academic Supervisor

Lazar Sandev

Introduction

In the liberal framework, the concept of 'rights' is understood in terms of need that is perceived by those who demand it as legitimate, and, therefore, the state has a responsibility to provide it for each and every citizen. Every democratic society ensures these rights, proclaiming them as fundamental principles, in most cases, writing it down on a legal document – the constitution. The principle of Freedom of Expression is probably the most complex and controversial of all constitutional guarantees.

The claim that citizens have rights that the state or the government is obliged to fulfil does not mean that the state may not, under certain circumstances, override these rights. In most cases, the state can limit that right in order to prevent a threat to public order, the security of the state, or third parties in need of protection, such as vulnerable categories of citizens (e.g. children). The problem becomes more controversial in nowadays' society where the Right to Freedom of Expression is predominantly exercised online. This constitutes new challenges regarding the issue of internet censorship and access to information.

This research elaborates the boundaries of free speech and communication on the Internet platforms and the mechanisms for protecting this rights through analysis of the Republic of North Macedonia's national legislation framework (or the absence of it.), aiming to detect if the methods that the country is using are sufficient for keeping the balance between safeguarding and surveillance in the modern era of technologies.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

Freedom of Expression as a fundamental principle is primarily provided in the state's highest legal act – the **Constitution of the Republic of North Macedonia (Устав на Република Северна Македонија)**. The Constitution provides for extremely broad protection of this right and guarantees all its aspects and forms. In Article 16, paragraph (1) the freedom of conviction, conscience, thought and public expression of thought is guaranteed. In the following paragraph of the same Article the freedom of speech, public address, public information and free establishment of institutions for public information is guaranteed.[1594]Paragraph (3) guarantees free access to information

[1594] Constitution of the Republic of North Macedonia ('Official Gazette of the RNM' no.52/1991).

and the freedom to receive and impart information.[1595] Therefore, the first part of this provision guarantees free access to information as an integral part of the Right to Freedom of Expression. This right is an integral part of the Right to Freedom of Expression because, without the guarantee of receiving information, there can be no free dissemination of it through the media. While not explicitly stated in the provision, access is guaranteed only to public information. Information not covered by this guarantee is primarily classified information, as well as those treated as personal data. The Constitution prohibits censorship[1596], even though it does not define it. There aren't any other constitutional provisions referring to censorship. The Constitution is extremely liberal and prohibits censorship in any form for the achievement of any purpose.

The Freedom of Expression is also protected by the international legal documents ratified by the Assembly of the Republic of North Macedonia, the European Convention on Human Rights (ECHR)[1597]; Universal Declaration of Human Rights (UDHR)[1598]; and International Covenant on Civil and Political Rights (ICCPR)[1599].

The Freedom of Expression often can be in conflict with others constitutionally guaranteed rights, such as the dignity and honour of each person, the right to private life, freedom of religion and public expression of religion[1600] and freedom of association, as the programs and activities of associations of citizens and political parties cannot be directed at violent destruction of the constitutional order of the Republic and at encouragement or calling upon military aggression or incitement to ethnic, racial or religious hatred or intolerance[1601].

1595 ibid.

1596 ibid.

1597 Council of Europe, European Convention on Human Rights, as amended by Protocols Nos. 11 and 14, 4 November1950, ETS 5, available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf, Article 9, 10, ratified 10 April 1997. [accessed 10 February 2020].

1598 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217, A (III), available at:https://www.un.org/en/universal-declaration-human-rights/ , Article 18, 19.[accessed 10 February 2020].

1599 UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, page 171, available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, Article 19, ratified 1994. [accessed 10 February 2020].

1600 Constitution of the Republic of North Macedonia ('Official Gazette of the RNM' no.52/1991) Article 19.

1601 Constitution of the Republic of North Macedonia ('Official Gazette of the RNM' no.52/1991) Article 20.

The most important laws related to Freedom of Expression are the Law on Media[1602], the Law on Audio and Audiovisual Media Services[1603] and the Law on Civil Liability for Insult and Defamation[1604]. Legal provisions that fall within the broader area of the Right to Freedom of Expression are also prescribed in the Criminal Code[1605], the Law on Classified Information[1606], the Law on Free Access to Public Information[1607], etc.

The Law on Media (Закон за медиуми)[1608] in Article 3 paragraph (1) guarantees the Freedom of Expression and the freedom of the media. It is important to note that with the amendments made on the Law in 2014 the terms 'electronic publications' and 'other electronic mediums' are deleted, and therefore are not subjected to these legal norms. We can come to the conclusion that the current state does not regulate Internet expression. The following paragraph defines what constitutes the Freedom of Expression of the media: the Freedom of Expression of thought, independence of the media, freedom to gather, research, publish, select, and disseminate information in order to inform the public, pluralism and diversity of the media, freedom of information flow and openness of the media to different opinions, beliefs and diverse content, access to public information, respect for human individuality, privacy and dignity, freedom to establish legal entities to perform the business of public information, printing and distribution of print media and other media from home and abroad, production and broadcasting of audio/audiovisual programs, independent editor, journalist, authors or creators content contributors or programmers; and other persons in accordance with the rules of the profession. Paragraph (3) stipulates that the freedom of the media can be restricted only in accordance with the Constitution of the Republic of North Macedonia. In Article 4, paragraph (1) the legislator prohibits publishing or broadcasting,

1602 Law on Media ('Official Gazette of the RNM' no.184/2013 and 13/2014).

1603 Law on Audio and Audiovisual Media Services ('Official Gazette of the RNM', no.184/2013, 13/2014, 44/2014, 101/2014, 132/2014, 142/2016, 132/2017, 168/2018, 248/2018 and 27/2019).

1604 Law on Civil Liability for Insult and Defamation ('Official Gazette of the RNM' no.143/2012).

1605 Criminal Code ('Official Gazette of the RNM' nos. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 and 248/2018). Decisions of the Constitutional Court of the RNM: U. no. 220/2000 dated 30 May 2001, published in the 'Official Gazette of the RNM' no. 48/2001; U. no. 210/2001 dated 06 February 2002, published in the 'Official Gazette of the RNM' no. 16/2002; U. no. 206/2003 dated 09 June 2004, published in the 'Official Gazette of the RNM' no. 40/2004; U. no. 228/2005 dated 05 April 2004, published in the 'Official Gazette of the RNM' no. 50/2006; and U. no. 169/2016 dated 16 November 2017, published in the 'Official Gazette of the RNM' no. 170/2017

1606 Law on Classified Information ('Official Gazette of the RNM' no.257/19).

1607 Law on Free Access to Public Information ('Official Gazette of the RNM' no.101/19).

1608 Law on Media ('Official Gazette of the RNM' no.184/2013 and 13/2014).

content in the media which endangers national security, encourages violent destruction of the constitutional order of the Republic of North Macedonia, invokes military aggression or armed conflict, incites or spreads discrimination, intolerance or hostility, based on race, sex, religion or nationality. The next paragraph provides that the special injunctions referred to in paragraph (1) of this Article shall be in accordance with the practice of the European Court of Human Rights. In Article 17 the right to correct published information guaranteed. Paragraph (1) of the Article states that everyone has the right to ask a media outlet, or editor-in-chief for a media outlet, to publish, without remuneration, a correction of published information stating inaccurate facts published in the information that infringe upon his rights or interests. Legal subjects and other organisations and bodies are also entitled to redress if their rights or interests are infringed by the information. A correction may also be required when the information has been published by a media publisher that has ceased to exist in the meantime. The person submitting the correction request has the right to request from the publisher of that medium or his legal successor, at his own expense, to publish the correction in another medium which is similar to the level of viewership/listening or circulation.[1609]In the case of scientific or artistic criticism, no right of correction is granted unless it corrects only incorrect facts.[1610]If the editor-in-chief of the media publisher fails to publish the correction in a manner and within the time limits specified in this Law, the person concerned shall have the right to file a complaint against the chief editor with the competent court within 30 days of the expiration of the correction deadline. That is, from the day when the correction was not published or was published in a manner not in accordance with this Law. The application for correction to the editor-in-chief is obligatory, and the person can not apply to the Court without such application for correction. The litigation regarding the announcement of the correction shall be resolved in the urgent procedure. The editor-in-chief shall be obliged when announcing the correction after the completion of the court procedure to state that the announcement is made on the basis of a final court verdict and is obliged to cite the pronounced verdict.[1611]

Subject to the regulation of **the Law on Audio and Audiovisual Media Services (Закон за аудио и аудиовизуелни медиумски услуги)** are the rights, obligations and responsibilities of broadcasters (primarily radios and televisions). Among the stated goals of this law is the promotion of Freedom of Expression. Article 48 paragraph (2) from this Law stipulates that the limitations

[1609] Law on Media, Article 22.
[1610] Law on Media, Article 17(4).
[1611] Law on Media, Article 23.

to Freedom of Expression shall be in accordance with the practice of the European Court of Human Rights[1612]. Unfortunately, this Law does not refer to the Internet.

The Law on Civil Liability for Insult and Defamation (Закон за граѓанска одговорност за клевета и навреда)regulates the Freedom of Expression. The Law applies to everyone, not only to the media. In its basic principles, the Law guarantees the Freedom of Expression and information as one of the essential foundations of the democratic society.[1613]Article 2, paragraph (2) provides that the restrictions on the Freedom of Expression and information shall be legally regulated by setting out strict conditions concerning the civil liability for insult and defamation, pursuant to the European Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights. In Article 6, paragraph (1) and (2) is regulated liability for insult stating that a person shall be liable for insult if he/she, with the purpose of humiliating, by means of a statement, behaviour, publication or in any other manner, expresses a demeaning opinion for another person that harms his/her honour and reputation. Furthermore, liability for insult shall also exist if, by such an activity, the reputation of a legal entity (legal person), a group of persons or a deceased person is tarnished. Article 7 stipulates the provision regarding the exemption of liability for insult. Paragraph (2) states that a person shall not be held liable for expressing a humiliating opinion for another person in a scientific, literary or artwork, in serious criticism, in the course of performing an official duty, journalistic profession, political or other social activity, in the defence of the freedom of public expression of thought or other rights, or in the protection of the public interest or other justified interests if: 1) from the manner it has been expressed or from the other circumstances, it follows that it does not have the meaning of an insult; 2) it has not caused significant harm to the honour and reputation of the person, and 3) it has not been presented exclusively with the intention to humiliate the personality of the other person or to degrade his/her honour and reputation. Furthermore, in the following paragraph, it is provided that a person shall not be held liable for expressing a humiliating opinion of a public office holder on a matter of public interest, if he/she proves that it is based on truthful facts, or if he/she proves that he/she has had a reasonable ground to believe in the truthfulness of such facts, or if the statement contains a justified criticism or it provokes a debate of public interest or if it has been presented in accordance with the professional

[1612] Law on Audio and Audiovisual Media Services, Article 48(2).
[1613] Law on Civil Liability for Insult and Defamation, Article 2(1).

standards and ethics of the journalistic profession.[1614]In the consideration of the circumstances for exemption from liability, the court shall apply the criteria for justifiable restriction of the Freedom of Expression contained in the European Convention on Human Rights and the case law of the European Court of Human Rights.[1615] Regarding the liability for defamation, the Law states that a person shall be held liable for defamation if he/she presents or disseminates false facts damaging the honour and reputation of another person with an established or apparent identity before a third party, with the intention of harming his/her honour and reputation while knowing or has been obliged to know and may know that the facts are false. Liability for defamation shall also exist if the false statement contains facts harmful to the reputation of a legal entity, a group of persons or a deceased person. If the presentation or dissemination of false statements of facts has been made by a mass medium (newspapers, magazines and other print media, TV and radio programs, electronic publications, teletext, and other forms of editorial program contents that are published, that is, broadcasted on a daily basis or periodically, in the form of a text, sound or image, in a manner which is accessible to the general public), the author of the statement, the editor or the person replacing him/her in the mass medium and the legal entity may be held liable for defamation. Even though the term 'other forms of editorial program contents' mentioned above, can be applied on the Internet predominantly, there is a great discussion regarding the matter. Upon filing the complaint, the plaintiff shall have the freedom to decide against whom of the persons referred to in this paragraph it shall file a lawsuit for determination of liability and compensation for damage caused by the defamation. The publisher, the editor or the person replacing him/her in the mass medium and the legal entity that publishes the mass medium, shall be held liable for defamation made by a journalist in the respective mass media who is the author of the statement, based on the principle of presumed liability.[1616] Article 9 states that the defendant shall be obliged to prove the truthfulness of the facts contained in the statement. The defendant that proves the truthfulness of his/her statement or proves the existence of reasonable ground to believe in its truthfulness shall not be held liable for defamation. As an exception to the previous provisions, the burden of proof shall fall upon the plaintiff who, as a public office holder, has a legal obligation to provide an explanation of specific facts which are related in the most direct way to, or are important for, the performance of his/her office, provided that the defendant proves that he/she has had reasonable grounds to present the

[1614] Law on Civil Liability for Insult and Defamation, Article 7(3).
[1615] Law on Civil Liability for Insult and Defamation, Article 7(5)
[1616] Law on Civil Liability for Insult and Defamation, Article 8.

statement in the public interest. Proving the truthfulness of facts related to the private life of the plaintiff shall not be allowed, unless the presentation of such facts has been made in a scientific, literary or artwork, in serious criticism, in the course of performance of official duty, journalistic profession, political or other social activity, in the defence of the freedom of public expression of thought or of other rights, or the protection of the public interest. If the defamation constitutes a public imputation against another of having committed a criminal offence or of being convicted of such an offence, the liability shall be exempted if the statement has been made in the public interest and if the person that has made it proves its truthfulness or proves that he/she had a reasonable ground to believe that those facts are true.[1617] As for liability for the electronic publications, the Law provides that the editor of an electronic publication shall assume the liability, along with the author, for compensation for the damage caused by the provision of access to insulting or defamatory information[1618]. The definition of the editor of an electronic publication is according to the Law on Media, 'the editor-in-chief leads the realisation of the contents that are published, i.e. broadcasted and is responsible for any information published in the media in accordance with the law'.[1619]The editor of the electronic publication shall not be held liable for the stated insult or defamation resulting from the provision of access to insulting or defamatory information if he/she proves that: 1) the author of the information published in the electronic publication has not acted under direct or indirect control or influence of the editor of the electronic publication and; 2) he/she has not been aware nor should have been aware that an insulting of defamatory material has been published in the electronic publication or, within a period of 24 hours after becoming aware of the insulting and defamatory character of the published text or information, he/she has taken all technical and other measures to remove that information. A request for removing information may also be filed by the aggrieved party[1620].

It is important to mention that the Law on Civil Responsibility on Insult and Defamation, as stated in the title of the law, only regulates civil responsibility. The Republic of North Macedonia in 2012 decriminalised the insult and defamation as offences, excluding the penal liability. However, the Criminal Code defines and sanctions hate-speech and hate crimes. In Article 394-d from the Criminal Code, hate speech expressed through computer systems, but also through public media is sanctioned from one year to five years' prison.

[1617] Law on Civil Liability for Insult and Defamation, Article 9.
[1618] Law on Civil Liability for Insult and Defamation, Article 11(1).
[1619] Law on Media, Article 8 (2).
[1620] Law on Civil Liability for Insult and Defamation, Article 11(2).

The right to free access to information as an integral part of the Right to Freedom of Expression is elaborated in the **Law on Free Access to Public Information (Закон за слободен пристап до информации од јавен карактер).** This Law regulates the conditions, manner and the procedure for exercising the right to free access to public information held by the state authorities and other bodies and organisations defined by law, the bodies of the municipalities, the City of Skopje and the municipalities of the city of Skopje, the institutions and public services, the public enterprises, the legal entities and natural persons that exercise public authorisations defined by law and activities of public interest and political parties in the part pertaining to revenues and expenditures.[1621] The Law in its provision grants free access to information to all legal entities and natural persons. Foreign legal entities and natural persons also have free access to information in accordance with this and other law[1622]. In Article 6 of the Law are stipulated the exclusions from free access to public information. That is information which, based on the law, represents classified information with an adequate degree of classification; personal data the disclosure of which would mean a violation of personal data protection; information the disclosure of which would mean a violation of the confidentiality of the tax procedure; information acquired or compiled for the purposes of an investigation, a criminal or misdemeanour procedure, for conducting an administrative or civil procedure, and the disclosure of which would have harmful consequences for the course of the procedure; information that endangers the rights arising from industrial or intellectual property (patent, model, sample, trademark and service mark, the designation of origin of the product). The information excluded from free access shall become available when the reasons for their unavailability cease to exist.

When it comes to other mechanisms for protection from limitation towards Freedom of Expression, the Constitution in Article 110, in addition to the other enumerated competences of the Constitutional Court, stipulates that the Constitutional Court also protects the freedoms and rights of the individual and citizen relating to the freedom of conviction, conscience, thought and public expression of thought, political association and action, and prohibition of discrimination of citizens on the grounds of sex, race, religious, national, social and political affiliation. Therefore, our constitutional system has not introduced a comprehensive constitutional complaint as a remedy for the protection of human rights and freedoms but has provided for the protection of *strictu sensu* defined rights and freedoms by submitting a request for protection of human

[1621] Law on Free Access to Public Information, Article 1(1).
[1622] Law on Free Access to Public Information, Article 4.

and civil rights and freedoms to the Constitutional Court, including Freedom of Expression. Other constitutional rights and freedoms cannot be protected by this remedy, and the Court will reject such claims. This type of jurisdiction foresees not only administrative but also judicial decisions and actions of public authorities. The conditions for submitting a request for protection of rights and freedoms under Article 110 paragraph (3) of the Constitution, its elements, and the procedure before the Court are set out in the Rules of Procedure of the Constitutional Court.[1623]According to Article 51 of the Rules of Procedure of the Constitutional Court of the Republic of Northern Macedonia, every citizen who believes that an individual legal act or action has violated his/her rights and freedoms set out in Article 110, paragraph (3) of the Constitution of the Republic of North Macedonia may require protection from the Constitutional Court within two months from the date of submission of the final or effective individual legal act, or from the day of finding out about the action taken with which the violation occurred, but no later than five years from the date of its takeover. It is important to note that this right can only be exercised by citizens, meaning that the legal entities, thus media, other organisations and bodies do not have the equal status regarding the right to protection against the limitation of their Freedom of Expression. The status inequality regarding the right to request for protection of rights and freedoms under Article 110 paragraph (3) of the Constitution is considered as a disadvantage, especially regarding the media which The European Court of Human Rights refers to as a Fourth Estate or fourth power by analogy with the three traditional powers in a democracy (legislative, executive and judicial). It is also important to note that, until the writing of this report, the Court has not made a positive decision which found a violation of submitted requests for protection of the public expression of thought.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

North Macedonia is part of those countries that have no specific legal framework aimed at the blocking, filtering and takedown of illegal internet content and there is no legislative or other regulatory system put in place by the state with a view to defining the conditions and the procedures to be respected by those who engage in the blocking, filtering or takedown of online material.

[1623] Rules of Procedure of the Constitutional Court of the Republic of North Macedonia ('Official Gazette of the RNM' no.70/92 and 202/19).

The Republic of North Macedonia has traditionally only regulated broadcasting - that is, audiovisual media services. With the Law on Audio and Audiovisual Media Services and the Law on Media, such practice has changed. The Law on Audio and Audiovisual Media Services, unlike similar legal solutions in the neighbouring countries, does not mention internet media or electronic publications at all. It remains to be seen whether the possibility of incorporating online media into the legislative framework will be considered at some future stage of changes in the law, especially if it is known that the amendments to the EU Audiovisual Media Services Directive, which Macedonian legislation should align, plans to include at least some of the audiovisual content available through video exchange platforms.[1624]

The Law on Media was enacted in 2013 and was once considered unnecessary by the media community, as all matters pertaining to the print and online media sphere need to be regulated by their own regulations. The law introduces a clear obligation for registering the print media, obligations related to transparency of ownership and publishing a report to the public for the financial results that are achieved, but originally the intent was to impose such obligations for the online media, like our neighbouring Balkan countries have done it, such as Croatia. The definition of media is given in Article 2 of the Law on Media: 'Media are means of public information, i.e. any kind of media communication, such as newspapers, magazines, radio and television programs, teletext, and other means of daily or periodical publishing of editorially shaped content in written form, sound or image, in order to inform and meet the cultural, educational and other needs of the general public. Media are not newsletters, catalogues or other forms of publications, independent of the means of publication intended solely for advertising, educational system or business correspondence, for the operation of companies, institutions, associations, political parties, state and judicial authorities, public enterprises, legal entities with public authority and religious organisations. The newspapers and bulletins of the educational institutions, the 'Official Gazette of the Republic of North Macedonia', the publications of the units of local self-government, posters, leaflets, prospectuses and banners'[1625] are not considered as media, which means that the term internet media is explicitly excluded from its term and electronic publications. That is to say, the online

[1624] 'Internet Freedom in Macedonia': <https://metamorphosis.org.mk/wp-content/uploads/2018/09/Sloboda-na-internet-vnatresni-%D0%9C%D0%9A.pdf>, accessed 20 May 2020.

[1625] Law on Media: <http://mdc.org.mk/wp-content/uploads/2014/05/Zakon-za-mediumi_-prechisten-tekst.pdf>, accessed 20 May 2020.

media is out of any regulation in the special media legislation of the Republic of North Macedonia.

In Article 4 named Special prohibitions 'The publishing, i.e. transmission of media content must not threaten the national safety, call for the violent destruction of the constitutional order of the Republic of Macedonia, call for military aggression or armed conflict, incite or spread discrimination, intolerance or hatred based on race, sex, religion or nationality.' Because this is a general prohibition for publishing such content, we can conclude that the same provision should be valid for posting such content online.

The Article 17, named 'The right to correction to published information', states the following: 'Everyone has the right to ask from the media publisher, or from the Editor-in-Chief of the media publisher, free of charge, to publish a correction of the published information, which notes incorrect facts, published in the information, violating his/her rights or interests. Legal entities and other organisations and bodies also have the right to correction, if their rights and interests were violated with the information.'

Because in this Article the term media is generally used, we consider that in this case the obligation to correct inaccurate information also applies to the internet media, as nothing concrete is indicated. This section of The Media Act is rarely applicable, so there is not any relevant case law.

The use of copyright without allowance in the Republic of North Macedonia is punishable with the Law of copyright and other related law. The copyright and other related rights are under criminal, civil and offence protection. The media, including those on the Internet, are not excluded from legal liability. An Internet-portal, in a case of using of some photo, audiovisual piece, piece of some figurative art, written piece, music piece and some other copywritten pieces, must name the author and the place where it has taken the copywritten piece from.

Law on Insult and Defamation[1626] provides, among other things, liability for insult and defamation committed through electronic publications. Article 11 also provides responsibility for the editor of the electronic publication, together with

[1626] Law on Insult and Defamation: <http://mdc.org.mk/wp-content/uploads/2014/05/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD-%D0%B7%D0%B0-%D0%B3%D1%80%D0%B0%D1%93%D0%B0%D0%BD%D1%81%D0%BA%D0%B0-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%BD%D0%BE%D1%81%D1%82-%D0%B7%D0%B0-%D0%BD%D0%B0%D0%B2%D1%80%D0%B5%D0%B4%D0%B0-%D0%B8-%D0%BA%D0%BB%D0%B5%D0%B2%D0% B5%D1%82%D0%B0-1.pdf >, accessed 20 May 2020.

the author. In Article 14 paragraph 1 of the same law 'If the insult or defamation was committed by means of the mass media or a computer system, the injured party has the right to submit a request for publication of a reply, disclaimer or correction within seven days of the day he learned that is published, but not later than one month after its publication.' This means that the published content will be subject to correction, or additional disclaimer of what has already been published, but there is no duty to take down such content. In the same law in the part named Provisional Judicial Section, specifically in Article 23 '(1)By filing a claim for liability and compensation for damages, the injured party may submit to the competent court a request for a determination of an interim court order which consist a prohibition for further publication of abusive or defamatory statements. (2)The request should contain grounds of belief indicating the offensive or defamatory nature of the statement and its harm to the honour and reputation of the injured party.' As can be seen from the Articles above, there is the option for demanding and editing already published content and prohibiting further posting.

Our country has not been a party to a case related to blocking and takedown of internet content.

It is general knowledge that we have difficulties taking down internet content by private lawsuits due to the fact that internet portals (media, blogs) were not defined as legal persons who can be held liable as the traditional media. This legal issue did not have a unified implementation in all Appellate areas in the legal system. Only the Appellate area of Skopje (our capital) constituted legal precedent that all forms of internet portals cannot be held liable for civil responsibility because they cannot be defined as the traditional media and all lawsuits were dismissed on that ground. Such practise was dismissed in the meeting of the four Appellate courts in 2019.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

As previously mentioned North Macedonia does not have specific legal framework regarding blocking, filtering and takedown of illegal internet content so there are no actual grounds on which internet content can be blocked/filtered or taken down.

With regard to civil law in the Law on Civil Liability for Insult and Defamation[1627], the Basic Principles guarantee the Freedom of Expression and information as one of the essential foundations of a democratic society, while limiting the Freedom of Expression. In Section 3 in Article 13 which reads '(1) Before filing a claim for damages, the person or legal person to whom the damage made by insult or defamation is referred, is taking measures to mitigate the damage, with a request for an apology and public withdrawal. (2)The apology or public withdrawal of the statement referred to in paragraph 1 of this Article shall be published in the same place and in the same circumference in the printed media or on the Internet, or at the same time and in the same volume in the electronic media or website, as well as the information to which it responds (title, headline, subheading, text in written media or website, newsletter announcement, attachment).' Therefore, pursuant to this Article if the content is published through the mass media or a web site is offensive, in order to compensate the injured party, it may be withdrawn.

Our country does not have safeguards to ensure a balance between censoring and Freedom of Expression. But since we have ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms and it has direct application in our legislation, then its provisions will be applied in that case.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In our country, the issue of blocking and taking down internet content is not self-regulated by the private sector. There aren't any kind of measures or soft law related to this issue.

[1627] Law on Insult and Defamation: <http://mdc.org.mk/wp-content/uploads/2014/05/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD-%D0%B7%D0%B0-%D0%B3%D1%80%D0%B0%D1%93%D0%B0%D0%BD%D1%81%D0%BA%D0%B0-%D0%BE%D0%B4%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%BD%D0%BE%D1%81%D1%82-%D0%B7%D0%B0-%D0%BD%D0%B0%D0%B2%D1%80%D0%B5%D0%B4%D0%B0-%D0%B8-%D0%BA%D0%BB%D0%B5%D0%B2%D0%B5%D1%82%D0%B0-1.pdf>, accessed 20 May 2020.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

North Macedonia's operating legal system is one of the most liberalised[1628] in Europe in relation to maintaining a structural differentiation regarding the rights and duties, as well as the scope of the 'right to be forgotten' and 'the right to delete', as part of the extensive interpretation of the terminological integration of the internet censorship concept, *per se*.

The Macedonian legislator regulates the protection of personal data as fundamental freedoms and rights of natural persons, and in particular, the privacy rights related to the processing of personal data through the Law on Personal Data Protection. The current Law on Personal Data Protection fully regulates the fundamental right to protection of personal data, although new harmonisation will be required under European directives and regulations. The Macedonian Republic has ratified Convention no. 108/81 on the protection of natural persons, which refers to the automatic processing of personal data of the Council of Europe. At the moment, after the election process and the constitution of the Assembly, the adoption of the new Draft Law on Personal Data Protection is being prepared, which regulates the protection of personal data as fundamental freedoms and rights of individuals, and especially the right to privacy regarding the processing of personal data, in accordance with the aspiration to adapt to the new General Data Protection Regulation (EU) 2016/679 (GDPR). The current law on personal data protection provides an adequate definition of certain terminology that is of particular importance regarding the obtaining rights for the protection of personal data[1629], such as:

'Personal data' means any information relating to an identified natural or identifiable natural person, and a person who can be identified is a person whose identity can be identified directly or indirectly, especially on the basis of a personal identification number the citizen or on the basis of one or more features specific to his physical, physiological, mental, economic, cultural or social identity;

'Personal Data Processing' means any operation or set of operations performed on personal data in an automated or another manner, such as collecting, recording, organising, storing, adapting or modifying, retracting,

[1628] Article 16 of the Constitution of the Republic of North Macedonia states that Censorship is prohibited.
[1629] Law on Personal Data Protection (Official Gazette of the Republic of Macedonia No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 and 64/2018), Article 2

consulting, using, transferring, posting or otherwise making available, equalising, combining, blocking, deleting, or destroying;

'Personal Data Collection' is a structured set of personal data that is accessible in accordance with specific criteria, whether centralised, decentralised or disseminated on a functional or geographical basis.

'Personal data subject' is any natural person to whom the processed data relate;

'Controller of personal data collection' is a natural or legal person, a body of state authority or other body, which independently or together with others determines the purposes and the manner of processing personal data (hereinafter: controller). When the purposes and the manner of processing of personal data are determined by law or other regulation, the same law or regulation shall specify the controller or the specific criteria for its determination;

'Personal data collection processor' shall mean a natural or legal person or a legally authorised body of the state authority that processes personal data on behalf of the controller;

'Beneficiary' is a natural or legal person, a body of state authority or other body to which the data are disclosed.

'Consent of the personal data subject' shall mean a free and explicit statement of the personal data subject's consent to the processing of his personal data for predetermined purposes;

'Specific categories of personal data' are personal data that reveal racial or ethnic origin, political, religious, philosophical or other beliefs, membership in a trade union, and data relating to human health, including genetic data, biometric data, or data concerning sex life.

The law ascribes[1630] that the protection of personal data is guaranteed to any natural person without discrimination based on their nationality, race, skin colour, religious beliefs, ethnicity, sex, language, political or other beliefs, material status, birth, education, social origin, citizenship, place or type of residence or any other personal characteristics.

The main national body that 'takes upon the burden' to protect and advance the protection of personal data is the Directorate for Personal Data Protection. Any particular public authority, public institution, institutional establishment and other legal entity maintaining official registers, publicly available data sets or

[1630] ibid, Article 3-a

other data sets are obliged, free of charge, at the request of the Directorate for Personal Data Protection.

The Directorate may request assistance from the state administrative body responsible for the enforcement of the executive order[1631] if physical resistance or such resistance is justifiable to be expected, as in other cases provided for by law.

The Law on Personal Data Protection gives the Macedonian citizen the right to know what personal data the controllers collect, process and store about them and whether they work legally.

According to the Directorate for Personal Data Protection, the Right to be Forgotten is treated as Deleting Personal Data.

Prevention of the use of personal data

Regarding the Prevention of the use of personal data, every citizen has the right to request from the controller who keeps collections of personal data to stop processing the personal data that refer to him. There is no strict form that should be included and what the request should look like, but it is desirable to state this data:

- His/her identity and personal data to which they refer;

- When the processing of personal data is considered illegal;

- When personal data is used for another purpose and not for the one for which consent has been given;

- The possible harmful consequence of such processing;

- In what period is it desirable to stop processing their personal data (it should be a reasonable time).

It is recommended that a copy of the requests submitted to the controllers be kept, but also the responses received by the applicants, as well as the entire correspondence. They can be used as evidence in a dispute before a court or if a request is made to the Directorate.

Deleting personal data

Furthermore, the current Macedonian positive-legal regulations do not regulate strictu sensu, under which circumstances and factual conditions, the citizens can be covered under the veil of the 'Right to be Forgotten'. In this regard, the claim goes that the Macedonian national regulations are the most liberal in Europe in

[1631] Ministry of Interior Affairs of the Republic of North Macedonia

terms of the scope of the 'right to be forgotten' and 'the right to delete'. The adaptation of EU law, including the new GDPR and the case law of the ECtHR, is a process that has yet to conceptualise the visibility of the framework for the 'Right to be Forgotten'.

With regard to the Right to be Forgotten and deletion of personal data, every citizen has the right to request from the controller who keeps a collection of personal data, supplementing, amending or deleting his personal data, if they are incomplete, incorrect or not updated and if their processing is not in accordance with the law[1632].

To exercise this right, you need to submit a request to the controller. There is no special template in relation to how this request should look like, but in addition to the provided personal information, it is advisable to specify the personal data that a person would want to add, edit or delete, which is controlled by the controller.

It is recommended to keep a copy of the requests submitted to the controllers, but also of the answers received, as well as the overall correspondence with the controller. In case the controller determines that the personal data is incomplete, incorrect or not updated, he is obliged to add, change or delete it and within 30 days from the day of submitting the request to notify you in the writing.

Request for determination of a violation of the right to personal data protection (including the right to be forgotten)

Although the Right to be Forgotten is not stipulated as such in the current national legislation, if a person believes that their right to protection of personal data has been infringed, it can file a Request for Determination of a violation of the right to personal data protection. It is of due importance to notice that there needs to be a certain distinction between national and international prevailing of requesting wherefrom a personal data the citizen wants to be removed from. To this end, the person needs to provide personal information about him/her as well as the data about the controller that he/she believes that has violated their Right to Privacy. An application against an unknown controller cannot be filed, it needs to be strict and targeted. The scope of data that are needed in order to process the Personal Data Protection Directorate upon a person initiative is set as requests that are submitted to the Directorate. The Directorate for Personal Data Protection then decides upon a filled request form.

[1632] Article 14 of the Law on Personal Data Protection(Official Gazette of the Republic of Macedonia No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 and 64/2018)

Steps to complete the Application:

In the form, the natural person first specifies the personal data about them and the data of the controller (the name, that is, the name and surname of the controller who misused their personal data or you have information that he or she has acted contrary to the Law on Personal Data Protection).

Then briefly they describe what the injury is and what they have done so far, whether they have contacted the personal data protection officer with the controller and whether they have received a response from the controller for the specific case.

Enclose copies of correspondence between them and the controller, as well as other evidence if any.

Though there are not any specific regulations in relation to procedures of addressing the possibility to 'be forgotten' on international media sites and platforms, such as international social sites and search engines, wherefrom a party 'insists to be forgotten' and their personal information shared with the public, the Macedonian citizen mainly has three ways of addressing this issue:

1. To send a request 'to be forgotten' directly[1633] to the site or the search engine;
2. To send a request to the Directorate for Personal Data Protection so that they can proceed in the name of the citizen;
3. To inform the Ministry of Internal Affairs of the information that needs to be excluded from the public out of internationally penetrated sites and search engines, having in mind whether they are sensitive and they include confidential information or information that can harm the security or the national interest of the Macedonian Republic.

[1633] As noted in the Google Transparency Report where Google has made a register of Requests to delist content under European privacy law. Starting from May the 29th 2014, as of January the 1st 2020, Google has received 3,500,000 URLs requests from parties interested in delisting. The search engine must comply if the links in question are 'inadequate, irrelevant or no longer relevant, or excessive,' taking into account public-interest factors including the individual's role in public life. Pages are only delisted from results in response to queries that relate to an individual's name. The Report is available at: https://transparencyreport.google.com/eu-privacy/overview [accessed 13 February 2020]

6. How does your country regulate the liability of internet intermediaries?

According to the Organisation for Economic Co-operation and Development (OECD), 'internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit, and index content, products, and services originated by third parties on the Internet or provide Internet-based services to third parties'[1634] and lists the following organisations as fitting this definition:

1. Internet access and service providers (ISPs);
2. Data processing and web hosting providers, including domain name registrars;
3. Internet search engines and portals;
4. E-commerce intermediaries, where these platforms do not take title to the goods being sold;
5. Internet payment systems; and
6. Participative networking platforms, which include Internet publishing and broadcasting platforms that do not themselves create or own the content being published or broadcast.

The Internet is not a quite regulated area in the Republic of North Macedonia. The maxi is: what is regulated offline, should be regulated online. According to the national law of North Macedonia, the term 'internet intermediaries' is not defined, nor are there explicit legal provisions that regulate the responsibility of internet intermediaries. In the last years, efforts have been made to regulate part of the internet area. The Law on Civil Responsibility for Insult and Defamation, adopted in 2012, can be considered as a legal act that is closest to regulating online liability. But, the case law has not been equalised, so the Primary Court Skopje II – Skopje rejects the lawsuits for insult and defamation against internet portals, on the other hand, the Primary Court in Ohrid has passed verdicts confirmed by the Court of Appeal in Bitola which determine liability for non-pecuniary damage for insult and defamation from an internet portal.

In 2012, in the text of Pretext law on civil Responsibility for Insult and Defamation, a different legal statement for the responsibility of the internet service provider was incorporated, which raised different questions. In Article 11, line 1, it was said that the internet service provider takes responsibility, together with the author, for damage compensation made of access to insulting or defamatory information, as in Pretext law. Responsibility of provider

[1634] OECD , The economic and social role of internet intermediaries, april 2010.

provision of internet service had certain advantages, but weaknesses too. It would make order in offends or insult order via internet providers comments moderation. On the other hand, critics of this law saw an attempt of internet media censoring, because anyone who thinks is damaged could make a demand to erase some internet content. Anyway, after reactions of the public for Pretext Law, he was changed and in the final version, it has no responsibility for an internet provider, but for only for professional media.

The relationship between news aggregators and Internet portals and their responsibility is also important. News aggregators are news transmitters, ie a place where information can be obtained from multiple Internet portals. Accordingly the Law on Civil Responsibility for Insult and Defamation, there is no liability for insult if an opinion is conveyed. The question is whether there is a possibility to withdraw news from the news aggregator. In practice, the source of the information is first sought, and then the source is asked to withdraw the news directly, not from the news aggregator. This is important because under the Law on Civil Responsibility for Insult and Defamation, before filing a claim for damages, a natural or legal person who has been inflicted damage by insult or defamation takes measures to mitigate the damage, with a request for an apology and public withdrawal. The action or non-action of the one who should withdraw the news (source) is the basis for deciding on greater or lesser intangible damage.

In the 21st century, the Internet is the biggest source of information in the world and is the preferred choice for news ahead of newspapers, radio and television. Ergo, it has become embedded in every aspect of everyday human life. In most European countries, illegal downloading and file sharing is punishable by law. In North Macedonia, this kind of problems are not regulated yet, so internet users can download pirated content without any consequences. Macedonian internet services do not have a legal obligation to control what the Internet is being used for by their users. There is only a possibility to make regulations for this issue in the future.

The Right to Freedom of Expression is one of the most vital bases of one democratic society and one of the conditions for its progress. In democratic systems, every person has the right to express their opinion, to accept and transfer information and ideas, and this right should be functional.[1635]With internet development and new media, citizens got the possibility to create and

[1635] Institute of Human Rights. Realization the right to freedom of expression. Available from: http://civicamobilitas.mk/wpcontent/uploads/2018/02/Pravo_na_slobodata_na_izrazuvanje_MK_web.pdf[accessed 15 February 2020]

share online content. That is why Freedom of Expression online should also be considered from the aspect of how much is available on the Internet. It is important to emphasise that the right to freedom of speech is a powerful tool which can be misused and used to arise violence, spread hate and inflict of individual privacy and security. This misusage is much more possible via the Internet, especially in countries that have no regulations for internet content. There are no specific norms safeguarding the protection of the Freedom of Expression online. If a dispute arises the Courts or state authorities are obliged to implement the standards set out in the case law of the European Court of Human Right. We need to be guided by the maxim: what applies offline also applies online. Regarding Freedom of Expression, it is guaranteed in Article 16 of the Constitution of the Republic of Macedonia. Article 16 of the Constitution of the Republic of North Macedonia, reads as follows: 'The freedom of personal conviction, conscience, thought and public expression of thought is guaranteed. The freedom of speech, public address, public information and the establishment of institutions for public information is guaranteed. Free access to information and the freedom of reception and transmission of information is guaranteed. The right to reply via the mass media is guaranteed. The right to a correction in the mass media is guaranteed. The right to protect a source of information in the mass media is guaranteed. Censorship is prohibited.'[1636]

The Law on Civil Responsibility for Insult and Defamation guarantees the Freedom of Expression and information as one of the important grounds of a democratic society. Article 2 and 3 of this Law, stipulate that the limitations of the Freedom of Expression and information are legally regulated by determining of special conditions for civil responsibility for insult and defamation, in accordance to the European Convention for the protection of human rights and fundamental freedoms (Article 10) and the practice of the European Court of Human Rights. If the court, by the application of the provisions of this law cannot solve a certain question that is connected with the determination of the responsibility for insult or defamation, or if the court holds the opinion that there exists a legal gap or a conflict of the provisions of this law with the European Convention for the protection of the basic human rights, based on the principle of its priority over the domestic law, will apply the provisions of the European Convention for protection of the basic human rights and the practice of the European Court of Human Rights.[1637]

It can be concluded that the European Convention on Human Rights and the European Court of Human Rights case law will apply in terms of the balance

[1636] Article 16, Constitution of North Macedonia.
[1637] Article 2 and 3, Law on Civil Responsibility for Insult and Defamation.

between the protection of Freedom of Expression and the right to honour and reputation (Article 10 Versus Article 8 of the European Convention on Human Rights).

Any citizen who feels that has violated his Freedom of Expression there is a constitutional possibility under Article 110 of the Constitution of the Republic of North Macedonia to request effective protection of Freedom of Expression. It is necessary to submit a request for the protection of freedoms and rights to the Constitutional Court. The procedure for submission of an application is regulated by the Rules of Procedure of the Constitutional Court. In the decision, the Constitutional Court will also determine the manner in which the consequences of the application of an individual act or action by which the right of thought and expression have been violated shall be eliminated.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, the liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

In the next five years, the Republic of North Macedonia will have to implement the EU acquis, due to the fact that we are expecting the country to open its accession talks with the European Union. Such implementation of regulation regarding blocking and take-down content or liability of internet intermediaries will be pursuant to the European Union's view.

Moreover, the interpretation of the regulations will be definitely in the light of the judgments of the European Court of Justice and the European Court of Human Rights.

For the blocking and takedown content, North Macedonia will definitely implement the Electronic Commerce Directive in the next five years. But some difficulties can arise, due to the fact, the internet portals (media, blogs etc.) will have to invest (financially) in equipment and human resources to fully implement the Directive. Also, a lot of people will abuse the new situation by registering internet sites on domains such as .com or .net or other providers and the state (courts and state authorities) will not be able to effectively fight against information that will be classified as hate speech, slander or false statements.

Regarding the liability of internet intermediaries, North Macedonia does not have any policy or intention to regulate it. This is maybe due to the fact that the intermediaries are only disseminating information. From our legal system and

court practise a person or entity who is disseminating information published by a third party (the source) cannot be held liable.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in the online environment? If not, what needs to be done to reach such balance?

'Only in a free state can everyone think what he wants and speak what he thinks' - a thought in which Spinoza says what each state should accomplish – the liberty. Because, according to him, the free man always acts honestly and never badly and insidiously. Spinoza said that every human being has Freedom of Speech– Freedom of Expression, belief and religion. These are the three basic human rights according to him. Talking about the period of the 16th century, the emphasis on this kind of freedom is a great advance. But, every right has its limit, and so does the Freedom of Expression. Everything above the limits can turn into hate speech.

8.1. Hate- speech

It is very important to make a difference between the Freedom of Expression and hate speech because where one's freedom ends, the freedom of the other begins. Hate speech involves expressing hatred for a particular group. It is used to offend a person through racial, ethnic, religious, or other groups to which that person belongs. Such speech generally seeks to condemn the individual or group or to express anger, hatred, violence, or contempt. All racist, xenophobic, homophobic, and other related declarations of identity-assaulting expression could be brought under the notion of hate speech. The European Court of Human Rights in its judgments concerning hate speech derives from this definition of hate speech or its understanding as speech encompassing 'all forms of expression that propagate, incite, promote, or justify hatred based on intolerance'.

More precisely, hate speech as a concept refers to a whole range of negative speech, ranging from a speech that expresses, incites, invokes or promotes hatred, to offensive words and epithets, and even (albeit questionable) extreme examples of prejudice. In addition to direct speech, hate speech includes many other forms of expression, such as public use of offensive symbols (e.g swastika); their explicit display of parades, protests, public addresses and the like; cross burning (this is characteristic of the Ku Klux Klan in the United States); burning flags; graffiti writing; glueing posters; distribution and dissemination of leaflets

with such content; the expression on TV and radio; and more recently, the expression on the Internet.

8.2. Hate- speech and the Internet

The Internet has become a new front for hatred. The anonymity and mobility provided by this means of communication have made the expression of hatred easy in a broad and abstract space that is outside the realm of traditional law enforcement. The message of hatred can now reach millions of people through a network that additionally enables previously diverse and fragmented groups to connect, producing a sense of community and shared identity. In its efforts to tackle Internet hatred, the Council of Europe in 2001 adopted the Cybercrime Convention[1638]which is the first multilateral treaty to seek to tackle cybercrime and increase cooperation between states by harmonising national laws and investigative techniques. In 2003, the Council of Europe adopted a separate Protocol on Internet Hate Speech, which has a twofold purpose: 1) to harmonise criminal law in the fight against racism and xenophobia on the Internet, and; 2) to promote international cooperation in this field. This Protocol considers racist and xenophobic material: any written material, image, or other representation of ideas or theories that advocate, promote, or incite hatred, discrimination, or violence against an individual or group of individuals based on race, colour, ancestors of either national or ethnic origin, as well as a religion if used as a pretext for any of these factors.

8.3. How is hate speech regulated in Republic of North Macedonia

The regulation of hate speech is different. Criminal law bans on hate speech are focused on criminalising abuses of Freedom of Expression that include incitement to violence or other violations of equal freedoms and rights of others or the expression of discriminatory treatment of others. According to the Criminal Code, hate speech is incriminated under specific conditions. Our Criminal Code stipulates that: stipulates that 'One who spreads the ideas of superiority of one race over another or promotes racial hatred or incites racial discrimination shall be punished with imprisonment of six months to three years.'[1639] Also, there is an incrimination about the hate speech using the computer system: 'A computer system that disseminates racist and xenophobic written material, images or other representations of an idea or theory through

[1638] The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks.

[1639] Criminal Code of North Macedonia 2017, article 417, paragraph 3

the computer to the public that promotes, promotes or incites hatred, discrimination, or violence against anyone a person or group based on race, colour, national or ethnic origin, as well as religious belief, will be punished by imprisonment of one to five years.'[1640] More specifically, Article 179 stipulates that 'Anyone who deliberately mocks the Macedonian people and members of communities living in the Republic of North Macedonia shall be punished with a fine.' While Article 319 provides '(1) The one who by coercion, harassing, endangering, mocking national, ethnic or religious symbols, damaging foreign objects, desecrating monuments, graves or otherwise will cause or incite national, racial or religious hatred, discord or intolerance, was sentenced to one to five years in prison. (2) A person who commits the crime referred to in paragraph 1 by abusing his or her position or authority or if such acts result in disorder and violence against persons or property damage to a large extent shall be punishable by imprisonment of one to ten years.'

There are no provisions in the Constitution of the Republic of North Macedonia that refer to the term 'hate speech', but it does provide protection against discrimination on several grounds by the Constitutional Court. However, in the current constitutional court practice, few cases can be found in which the court has ruled on protection against discrimination, and as far as hate speech as a form of discrimination is concerned, the Constitutional Court has so far not explicitly stated this issue. In the Constitution of the Republic of North Macedonia, there are no explicit restrictions on the Right to Freedom of Expression, so in constitutional and legal disputes the Constitutional Court has resorted to interpretations as to whether 'sanctioned action' has the meaning of 'public expression of opinion' or 'has lost the meaning of freedom of opinion. and a public expression of the thought that the Constitution guarantees and protects.'

Hate acts are criminal offences motivated by prejudice where the perpetrator deliberately selects a victim with a protected characteristic (discriminatory basis). Online hate crimes cover those crimes committed by electronic communications.

Although in the Republic of North Macedonia we have criminal offences that regulate hate speech, so far we have almost no legal practice.

Hateful blogs and sites are also a common method of spreading hatred and intolerance to certain groups or individuals. Blogs provide the opportunity for haters by selectively moderating anonymous comments to create a community

[1640] Criminal Code of North Macedonia 2017, article 394, paragraph d

that shares only negative comments and stereotypes about a particular group. Although social networks have rules of use that prohibit hate speech, Facebook and other social networks are full of hate-promoting sites, and even groups that directly incite violence. Some of them are very difficult to find because they are available only to friends of the site. Example: Facebook groups titled: 'I hate girls', Death to Gypsies.

8.4. What exactly means 'Countries that are enemies to the Internet?' and where is our country placed?

The first and most important factor is censorship. Censorship of websites, social networks, freedom of speech and writing, etc. - control of the publication and access to information found on the Internet. In many countries, such as China, Cuba, Syria, Saudi Arabia, North Korea and others, Internet censorship is commonly practised by their governments.

Internet (censorship) around the world is present in most countries around the world, but in different dimensions and with drastically different conditions. In the US, for example, Internet filtering occurs on computers mostly in libraries, schools, and similar establishments, while in China, for example, social networks such as Facebook, Twitter and the likes are completely banned and punishable by law. In France and Germany, content related to Nazism or Holocaust denial has been blocked. Child pornography, hate speech, and websites that promote intellectual property theft are blocked in many countries around the world.

8.5. Which are the positive measures that our country can prescribe against hate – speech?

It is better to prevent than to punish. So, positive measures are so much more effective than the punishments, bans and incriminations. International human rights standards highlight the importance of a range of positive policy measures states should employ alternatives to censorship, in order to more effectively address the root causes of 'hate speech.' States are obligated to create an enabling environment for Freedom of Expression and equality, to take positive steps to promote diversity and pluralism, to promote equitable access to the means of communication, and to guarantee the right to information. So, the authorities in the Republic of North Macedonia should take measures like this one, in order to protect human rights and to prevent violation of human rights and Freedom of Expression in general. So, here are some of the measures that could be useful in our society:

1. Creating collaborative networks to build mutual understanding, promote dialogue, and inspire constructive action in various fields;

2. Creating a mechanism within the government to identify and address potential areas of tension between members of different religious communities, and assist with conflict prevention and mediation;
3. Train government officials in effective outreach strategies;
4. Encourage efforts by leaders to discuss within their communities the causes of discrimination, and evolve strategies to counter them;
5. Speak out against intolerance, including advocacy of religious hatred that constitutes incitement to discrimination, hostility or violence;
6. Combat denigration and negative religious stereotyping, as well as incitement to religious hatred, including through education and awareness building;
7. Recognise that the open, constructive, and respectful debate of ideas plays a positive role in combating religious hatred, incitement, and violence;
8. Adopting a comprehensive public policy approach to tackling forms of intolerance and prejudice of which manifestations of 'hate speech' are symptomatic;
9. Building institutional knowledge, especially through creating properly-funded and independent equality institutions, with mandates to develop data collection mechanisms and to promote scientific research on discrimination is an important first step for identifying key actors and obstacles to change, and to arrive at priority areas for policy interventions;
10. Public education and information campaigns related to discrimination, especially in cases where discrimination is institutionalised and has a history of going unchallenged. Areas of priority may include schools, the medical profession, the armed forces, the police, the judiciary, and the Bar, as well as sport. It emphasises that cooperation with a broad range of stakeholders is necessary;
11. Strengthening the role of an independent, pluralistic, and self-regulated media: a model framework for the media should promote the right of different communities to freely access and use media and information and communications technologies for the production and circulation of their own content and for the reception of content produced by others. The media should also recognise the role they play in responding to 'hate speech,' and reflect the principle of equality in

voluntary professional codes of conduct, as well as taking effective steps to promulgate and implement such codes, including through effective self-regulatory mechanisms.

We are also aware of the power of the Internet as a place where everyone can share everything, including hate- speech. The proliferation of online 'hate speech' has been identified as a serious problem, and policy responses[1641] to it have posed certain challenges in terms of the protection of Freedom of Expression. There seems to be a reluctance to formulate specific and positive policies and approaches to promote pluralism through new media. Our country should dedicate resources and efforts in this area. These could include, for example:

1. Promoting and investing in digital literacy skills,[1642] so that a wide range of individuals understand the benefits of digital technologies, particularly online media, as well as the benefits of engagement and contributing information;

2. Initiatives to monitor media pluralism that should specifically include indicators relating to digital technologies, particularly as opportunities afforded by the Internet, convergence, blogging, social networking sites, mobile phones and other forms of electronic communication could result in monopolies of certain online platforms and create threats to media pluralism.

The media plays an important part in responding to 'hate speech' through promoting equality and non-discrimination, and the Right to Freedom of Expression. All forms of mass media should recognise that they have a moral and social responsibility to promote equality and non-discrimination and that could help to prevent hate speech. Equality and non-discrimination should apply to individuals with the broadest possible range of protected characteristics. In respect of their own internal practices, mass media entities should take steps to:

1. Ensure that their workforces are diverse, and representative of society as a whole;

1641 These policies should also address doubts about the capacity of the Internet-based media in particular, to offer an alternative, even a corrective to traditional media

1642 Digital literacy includes the development of the technical skills and abilities required to use digital technologies, as well as the knowledge and abilities needed to find, analyze, evaluate and interpret specific media texts, to create media messages, and to recognize their social and political influence. Multiple and complementary literacies are seen as essential for the exercise of rights and responsibilities in regard to communications; see UNESCO, World Trends in Freedom of Expression and Media Development: Special Digital Focus, 2015, available from https://bit.ly/20mQeXT.

2. Address, as far as possible, issues of concern to all groups in society, in particular women, minorities and people from all parts of the community;
3. Seek a multiplicity of sources and voices from within different communities, rather than representing communities as homogenous entities;
4. Adhere to high standards of reporting that meet recognised professional and ethical standards;
5. Promulgate and effectively implement professional codes of conduct for the media and journalists that reflect equality principles,[1643].
6. Take care to report in context, and in a factual and sensitive manner;
7. Ensure that acts of discrimination are brought to the attention of the public;
8. Be alert to the danger of discrimination or negative stereotypes of individuals and groups being furthered by the media;
9. Avoid unnecessary references to race, religion, gender, sexual orientation, gender identity and other group characteristics that may promote intolerance;
10. Raise awareness of the harm caused by discrimination and negative stereotyping;
11. Report on different groups or communities and give their members an opportunity to speak and to be heard in a way that promotes a better understanding of them, while at the same time reflecting the perspectives of those groups or communities;
12. Invest in and ensure access to professional development programs that raise awareness about the role the media can play in promoting equality and the need to avoid negative stereotypes. Public service broadcasters should be obliged to avoid negative stereotypes of individuals and groups, and their mandate should require them to promote intergroup understanding and foster a better understanding among the public of different communities and the issues they face.

[1643] Based on the Camden Principles, op. cit.; and ARTICLE 19, Media Diversity Institute and the European Federation of Journalists, Getting the facts right: reporting ethnicity and religion, 2012, available from https://bit.ly/1spL1Q6.

Civil society plays a critical role in advancing the protection and promotion of human rights. Their activities can be central in responding to 'hate speech,' as they can provide the space for both formal and informal interactions between people of similar or diverse backgrounds, and platforms from which individuals can exercise their Right to Freedom of Expression, and tackle inequality and discrimination. At local, national, regional and international levels, civil society initiatives are among the most innovative and effective for monitoring and responding to incidents of intolerance and violence, as well as for countering 'hate speech.' Civil society initiatives are often designed and implemented by the individuals and communities most affected by discrimination and violence, and provide unique possibilities for communicating positive messages and educating the public, as well as monitoring the nature and impact of discrimination. Ensuring a safe and enabling environment for civil society to operate is therefore also crucial.[1644] Public information and education campaigns are essential to creating an environment in which the sharing of information is maximised, and critical discourse can flourish. This is particularly the case when discrimination is institutionalised. Priority areas in this respect may include schools, the medical profession, the armed forces, the police, the judiciary, the Bar, as well as in sport. However, this also requires NGOs, equality bodies, religious institutions, police, policymakers and international organisations to collaborate on tackling manifestations of intolerance and prejudice in society.

Also, the Internet as a medium can be useful as a way of protecting against hate speech. So, here are the measures that can be done on the Internet:

What should ISPs do?

1. Define hate speech,
2. Prohibit hate speech on their site (location) through a clear statement within the User's Guide,
3. Establish clear, easily accessible mechanisms for users to report hate speech,
4. Act quickly removing or isolating hate speech online content, after being repeatedly reported, to inform users why their reporting of hate speech has been rejected,
5. Train authorised anti-racist and xenophobic materials on the Internet and other hate speech,

[1644] The Camden Principles on Freedom of Expression and Equality, ARTICLE 19, 2009, available from http://bit.ly/1XfMDrL. The Principles were developed with the participation of a high-level group of UN officials and representatives from other intergovernmental organizations.

6. Enact effective laws to combat hate speech online, including protection against cyber-harassment, to act responsibly on their sites, in order to prevent online hate speech,
7. publicly condemn online hate speech, not abuse the fight against online hate speech,
8. to restrict the Right to Freedom of Expression (in particular it is about content that is critical of the authorities).

Institutions in Macedonia have been deaf to calls for violence and hate speech on the Internet for years. Although we have everything set on paper, in reality, happens something different. But still, we must confess that something has been done. The Republic of North Macedonia speaks out against intolerance, including advocacy of religious hatred that constitutes incitement to discrimination. Also, Republic of North Macedonia organises public events and information campaigns related to discrimination in order to stop hate speech online. The Republic of North Macedonia has also a good legal framework for recognition and sanctioning of hate speech.

But, there are a lot of things that the Republic of North Macedonia should and will have to do, according to the previous rules. The Ministry of Interior does not have statistical data on hate speech at disposal, so they will have to start working on that. In cases of hate speech, the Public Prosecution does not act ex officio and also does not show any interest for adequate and timely action upon submission of criminal charges. The insufficient level of training when it comes to recognising and sanctioning hate speech on the part of police officers, judges, public prosecutors and lawyers, as well as lack of training provided by the relevant authorities. The Criminal Code does not stipulate alternative measures or sanctions for the perpetrators of hate crime. Those measures will be more effective and would reduce crime.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

Finding a balance between allowing Freedom of Expression online and protection against hate speech in the online environment is definitely one of the main issues for government authorities in the 21st century. Albeit, it is not the only right in need of balancing, but there are also other areas of conflicting interests that need to be addressed. The Council of Europe (to which, the

Republic of North Macedonia became the 38th member state in 1995[1645]) emphasises the need to balance Freedom of Expression and the Right to Private Life, freedom of thought, conscience and religion, freedom of assembly and association and the prohibition of discrimination.[1646]

Firstly, it is important to note that Freedom of Expression, as a fundamental human right, does not only entail the right to express your own opinion, but also the freedom to hold opinions and the right to obtain information. These elements are contained in Article 10 (1) of the ECHR, which states that:

'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises…'[1647] While this part expresses the rights related to Freedom of Expression, the following paragraph in the same Article, expresses the restrictions of this freedom, related to:

1. The interest of national security;
2. Territorial integrity or public safety;
3. Prevention of disorder or crime;
4. Protection of health and morals;
5. Protection of reputation or rights of others;
6. Prevention from the disclosure of confidential information;
7. Maintaining the authority and impartiality of the judiciary[1648].

9.1 Freedom of expression and the right to private life

In Article 8 of the ECHR, the right to respect for private and family life is guaranteed through the obligation this provision imposes that everyone respects one's private and family life, their home and their correspondence[1649]. This means that the exercise of the Freedom of Expression by one person should not be at the expense of another person's private and family life. While the Commissioner for Human Rights has underlined that Freedom of Expression must be guaranteed more effectively in criminal defamation proceedings[1650], the

1645 *Law on the ratification of Statute of Council of Europe*, Official Gazette of the Republic of Macedonia no53/1995 of 08.11.1995.

1646 Council of Europe, Guide to good and promising practices on the way of reconciling freedom of expression with other rights and freedoms, in particular in culturally diverse societies(Steering Committee on Human Rights (CDDH), Council of Europe, 2019) p 70.

1647 Council of Europe*, European Convention for the Protection of Human Rights and Fundamental Freedoms*, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, art 10 (1).

1648 iIbid, art 10 (2).

1649 ibid, art 8 (1).

1650 Council of Europe, Guide to good and promising practices on the way of reconciling freedom of expression with other rights and freedoms, in particular in culturally diverse societies, p 70.

legislature in the Republic of North Macedonia has taken up a different approach in this area.

The laws define the balance between the Freedom of Expression and the Right of Private Life (or the Right to Reputation – one's image). This applies to traditional media, online media, social platforms and natural persons.

The balance between the Freedom of Expression vis-à-vis the right to private life – reputation has been a severe problem in the past five years in North Macedonia. The problem was, mostly, the fact that the courts had a problem of defining the internet portals and blogs as parties in the civil proceedings. Namely, our country consists of 4 Appellate areas (Skopje, Gostivar, Bitola and Shtip). The Appellate areas of Gostivar, Bitola and Shtip did not have any legal problems of deciding on the liability of the internet portals with .mk domains, i.e. to treat them as traditional media. On the contrary, the Appellate area of Skopje had another legal view. They stated in their judgments that internet portals cannot be held liable for content on their web sites same as traditional media, because they did not have a publisher or editor in chief pursuant to the Law on Media.[1651] Such practise was in force until March 2019 when they adopted the legal opinions of the other Appellate courts in North Macedonia. Therefore, it is safe to conclude that there was no unified balance between the Freedom of Expression and the Right to Private Life (Right to Reputation) when it comes to the internet portals.

9.2 Freedom of expression and freedom of thought, conscience and religion

This second aspect is extremely important in pluralist societies, such as the one in North Macedonia, where many different religions coexist on the same territory. On the one hand, there is the right for a person to express their thoughts, have conscience and religion, the freedom to change their beliefs and to manifest them individually or together with others, as it is determined in the ECHR.[1652] On the other hand, this right imposes an obligation to respect other people's right to freedom of thought, conscience and religion. This right is covered by the Law on the legal personality of churches, belief communities and religious groups,[1653] where the freedom to manifest a religion or belief, individually or together with others, is recognised.[1654] The obligation to respect

1651 *Law on Media*, Official Gazette of the Republic of Macedonia no 184/2013 of 26.12.2013.
1652 European Convention for the Protection of Human Rights and Fundamental Freedoms, art 9 (1).
1653 Law on the legal personality of a churches, belief communities and religious groups,Official Gazette of the Republic of Macedonia no 113/2007 of 20.09.2007.
1654 Ibid, art 3.

other people's religion is set by prohibiting religious discrimination.[1655] Additionally, the more recent Law on prevention and protection against discrimination[1656] follows the previous anti-discrimination law rationale, by including religion and religious beliefs in the prohibited bases for discrimination[1657]. It can be concluded that the freedom of thought, conscience and religion is protected by these laws, but they do not specify what happens in the event of that right being breached by other people's right of expression online.

9.3 Freedom of expression and freedom of assembly and association

The freedom of assembly and association is a complementary right to the Freedom of Expression, meaning people have the right to form groups with other people with the same opinion and together they can express that opinion, in order to be better heard from the public authorities. This right is entailed in the ECHR as follows: *'Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.*'[1658] The purpose of this provision is to allow individuals and groups to come together to collectively address and resolve challenges and issues that are important to society,[1659] which is also especially important for pluralist societies such as the one in North Macedonia. In this context, there have been many examples of calls for public assembly through social media, such as Facebook, where people are free to express their opinions online and arrange peaceful protests and marches with other persons sharing their opinion on the matter. This concept was especially popular recently when marches against air pollution were organised, as well as protests for other causes, such as animal rights, labour rights, student rights, and protests for various political causes.

The main source of law dealing with freedom of assembly and association with others is the Law on public assembly[1660], which regulates how citizens can achieve their right of public assembly for the purpose of peaceful expression and public protest. In it, the Freedom of Expression is recognised through the right to group yourself with other people and express their opinion together, but it is not stated how this freedom of assembly could be realised through online platforms. Again, there is a need for reform in the area, especially because

1655 ibid, art 4 (1).

1656 *Law on prevention and protection against discrimination,* Official Gazette of the Republic of North Macedonia no 101/2019 of 22.05.2019.

1657 ibid, art 5.

1658 European Convention for the Protection of Human Rights and Fundamental Freedoms, art 11 (1).

1659 Council of Europe, Guide to good and promising practices on the way of reconciling freedom of expression with other rights and freedoms, in particular in culturally diverse societies, p 80.

1660 *Law on public assembly*, Official Gazette of the Republic of Macedonia no 55/1995 of 13.11.1995.

organising public assemblies online is becoming more and more popular in recent years.

9.4 Freedom of expression and prohibition of discrimination

In the second point of this section, it was analysed how religious discrimination is regulated in the Republic of North Macedonia. However, this is only one aspect from a much broader global issue – discrimination should be prohibited on any ground. The European Convention clearly states that the rights and freedoms provided by it shall be secured without discrimination on any ground. This particular provision includes '…*sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.*'[1661], as grounds for discrimination which are prohibited. The aforementioned Law on prevention and protection against discrimination in point 2, has included an even longer list of grounds for discrimination and thus, established solid grounds for protection of the citizens of North Macedonia from discrimination. However, this law does not mention how Freedom of Expression online and the prohibition of discrimination should achieve balance. It is clear that citizens should equal and that the rights of one of them should not be breached in order for another to enjoy their rights. So what happens in the event that one person discriminates against another using an online platform?

The Criminal Code[1662] of North Macedonia offers a solution particularly applicable to the use of computer systems. More precisely, the provision on spreading racist and xenophobic material by means of computer system states that: *'The person who through a computer system spreads resist and xenophobic written material, images or other representation of an idea or theory that assists, promotes or encourages hatred, discrimination or violence against any person or group based on their sex, race, skin colour, gender, membership in a marginalised group, ethnicity, language, citizenship, social origins, religion or religious persuasion, other types of persuasion, education, political affiliation, personal or social status, mental or physical disability, age, family or marital condition, property status, health condition or any other base envisaged with the law or ratifies the international agreement, shall be punished with imprisonment of one to five years.'*[1663]This Article contains the same grounds for discrimination included in the Law on prevention and protection against discrimination, consistently protecting the citizens of North Macedonia against discrimination conducted through a computer system. Additionally, this Article also includes punishment for persons perpetrating this

[1661] European Convention for the Protection of Human Rights and Fundamental Freedoms, art 14.
[1662] *Criminal Code*, Official Gazette of the Republic of Macedonia no 37/1996 of 29.07.1996.
[1663] ibid, art 394-g (1).

criminal act by abusing their position or authorisation, by allowing imprisonment of one to ten years.[1664] The Helsinki Committee for Human Rights in North Macedonia has been very active in invoking this Article before national courts and protecting citizens. However, further efforts are needed for the protection against discrimination, especially in culturally diverse societies such as the one in North Macedonia.

10. How do you rank the access to freedom of expression online in your country?

Information and Communication Technologies (ICTs) are defined as a blend of information technology and communication networks that enable telecommunications to be communicated electronically. The most well-known ICTs are the Internet and mobile phones. ICTs allow 'all ideas to be spread'[1665] and to connect geographically distant persons. Accordingly, the Internet has enabled the wide and free exchange of data and information, accelerating the development of what we began to call 'information society'. ICTs have become an indispensable tool for developing ideas and attitudes[1666]. They are real platforms for free expression and are often regarded as information carriers. These new participatory technologies make up a new space for Freedom of Expression.[1667]

As previously noted, in the Republic of North Macedonia there is no law of Freedom of Expression online yet, taking this fact in consideration the Freedom of Expression is at a high level, as well as the access to Freedom of Expression since the entire country is well covered with information technology network. This refers mostly to the new and young generations and less for the elderly generation that lacks internet knowledge in general.

In glace of the year 2019, many types of access Freedom of Expression are noticed, beside social media as one of the most accessible and easy to use tools for online expression, public web portals of different institutions and municipalities were made available for the citizens to express their opinions, give feedback and demand for more information. What is little to know is how these

[1664] ibid, art 394-g (3).

[1665] Luc GRYNBAUM, « Internet », in Dictionnaire des droits de l'homme, Quadrige- PUF, 2008, page 537.

[1666] According to a survey conducted by 2IDHP, 68% of respondents said they considered social networks as a source of information.

[1667] Freedom of Expression and Privacy in the Digital Age – Metamorphosis.

feedbacks were handled afterwards, the access is for sure granted but no guarantee how those expressions were taken into consideration.

There is one resolution that affirms that 'the same rights that people have offline must also be protected online, in particular, Freedom of Expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with Articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights'.[1668]

A number of cases confirm that the access of online Freedom of Expression is used for online hate speech, this is a consequence of the fact that in our country there is no judicial judgment.

The hate of speech is present on any level and age category, which brings us to misinterpretation of what truly means Freedom of Expression without breaching other human rights.

In every yearly and monthly report from the Helsinki Committee for Human Rights in North Macedonia, there are examples of reported cases of online threats and hate speech on social networks.[1669]

To give an example, there are over 660 hate speeches evidenced online from February 2014 till February 2020, on the social networks, where most of them are on 'Facebook' and 'Twitter' platforms.[1670]

Another specimen, on the international level, North Macedonia has the total score of 59.58% in 2019 where it has increased compared to 2017 and 2018 with 56% in the Freedom Barometer, and the average of 50% is retained in all other categories (presented by the Freedom Barometer), except for the Rule of Law category. The biggest increase was on the Freedom of Media from 3.60% in 2017 and 2018 to 6.83% in 2019.[1671]

These numbers lead as to think in a direction that maybe the Freedom of Expression online for political topics might be jeopardised by political influencers, parties or other sides involved in this area of functioning.

In the context of 'cybercrime', the Ministry of Internal Affairs of the Republic of North Macedonia recognises and extends the burning of racist and xenophobic materials through computers systems, as well as racist and xenophobic motivated threats and insults. In the July 2005 Republic of North

[1668] Freedom of Expression on the Internet – Council of Europe Publishing.
[1669] Yearly report of 2018 for hate speech from Helsinki Committee for Human Rights.
[1670] Website for reporting hate speech online – www.govornaomraza.mk.
[1671] Freedom Barometer – www.freedombarometer.org. Accessed 20 May 2020

Macedonia ratified Additional Protocol to the Convention on Cybercrime incrimination of racist and xenophobic acts by information systems.[1672]

Moreover, the above-stated examples are only emphasising the need for regulation of online expression, but only if they are violating wellbeing of others.

Regarding all of the researches listed above, we can conclude that the access to Freedom of Expression in North Macedonia is not excellent or very good, but is on the satisfactory level and on a scale from one to five, we can rank the access to Freedom of Expression in our country with number three.

11. How do you overall assess the legal situation in your country regarding internet censorship?

Although we have many laws that deal with what is happening in the world of the Internet, however, none of them elaborates on what Freedom of Expression means on the Internet and where its boundaries are. At the same time, we have the Criminal Code, which incriminates hate speech and hate crime. Nevertheless, it is often difficult to draw a line dividing Freedom of Expression in general, as well as that of the Internet and hate speech. Although we are guided by the premise, 'You have the right to speech but not hate speech'; yet, often we cannot decide where we should go and where our own boundaries are until someone else has set them. It seems that we do not have such legislation. Therefore, we need a systematised law that will elaborate on this topic in detail, define the Freedom of Expression on the Internet and delineate it with hate speech. This would achieve greater legal certainty and a certain cessation and reduction of hate speech and its emerging forms. At the same time, in order to prevent the full abuse of the Freedom of Expression, it is necessary to respect and apply the international legal documents ratified by our country (Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, International Covenant on Economic, Social and Cultural Rights, the European Convention for the Protection of Human Rights), which guarantee the Right to Freedom of Expression for the practical exercise of this right. The practice of the European Court of Human Rights and the Court of Justice of the European Union regarding the Right to Freedom of Expression and their proper application by all relevant institutions in the Republic of North Macedonia must be regularly followed, as a basis for amending the existing laws and the adoption of new laws as well as the basis for the administration of justice. It is necessary to amend the national legal framework in accordance with the conclusions drawn

[1672] Freedom on the Internet in North Macedonia – report from 2017 by Metamorphosis.

from this analysis in order to more effectively protect the Right to Freedom of Expression.

Conclusion

It is clear from the Macedonian legislation that as the Freedom of Expression is guaranteed, so are other rights, such as the right to private life, freedom of thought, conscience and religion, freedom of assembly and association and the prohibition of discrimination. However, although protected in theory, the question still remains how this protection is ensured in practice, having in mind the fact that there are not many cases in these areas. Additionally, legislation needs to be amended in order to achieve the necessary balance between the Freedom of Expression online, which would include the new technological means by which people communicate and express themselves. In general, we can conclude that our country protects the Freedom of Expression as a constitutional guarantee, making it one of the basic freedoms and rights of the individual and the citizen, which is a prerequisite for a democratic society. At the same time, the state prohibits censorship at any form and for the achievement of any purpose, thereby and internet censorship. Unfortunately, it is important to emphasise that our national legislation lacks regulations and clear provisions related to the safeguards to Freedom of Expression exercised online.

Table of legislation

Provision in Macedonian language	**Corresponding translation in English**
Устав на Република Северна Македонија,Член 16: (1) Се гарантира слободата на уверувањето, совеста, мислата и јавното изразување на мислата. (2) Се гарантира слободата на говорот, јавниот настп, јавното информирање и слободното основање на институции за јавно информирање. (3) Се гарантира слободниот пристап кон информациите, слободата на примање и пренесување на информации. (4) Се гарантитра правото на одговор во средствата за јавно информирање. Се гарантира правото на испаравка во средствата за јавно информирање. Се гарантира правото на заштита на изворот на информацијата во средствата за јавно информирање. (5) Цензурата е забранета.	The Constitution of the Republic of North Macedonia, Article 16: The freedom of personal conviction, conscience, thought and public expression of thought is guaranteed. The freedom of speech, public address, public information and the establishment of institutions for public information is guaranteed. Free access to information and the freedom of reception and transmission of information are guaranteed. The right to reply via the mass media is guaranteed. The right to a correction in the mass media is guaranteed. The right to protect a source of information in the mass media is guaranteed. Censorship is prohibited.
Устав на Република Северна Македонија, член 100: (1) Уставниот суд на Република Северна Македонија: - одлучува за согласноста на законите со Уставот; - одлучува за согласноста на другите прописи и на колективните договори со Уставот и со законите; - ги штите слободите и правата на човекот и граѓанинот што се однесуваат на слободата на уверувањето, совеста, мислата и јавното изразување на мислата, политичкото здружување и дејствување и забраната на дискриминација на граѓаните по основ на пол, раса, верска, национална, социјална и политичка припадност;	The Constitution of the Republic of North Macedonia, Article 100: The Constitutional Court of the Republic of Macedonia - decides on the conformity of laws with the Constitution; - decides on the conformity of collective agreements and other regulations with the Constitution and laws; - protects the freedoms and rights of the individual and citizen relating to the freedom of conviction, conscience, thought and public expression of thought, political association and activity as well as to the prohibition of discrimination among citizens on the ground of sex, race, religion or national, social or political affiliation; - decides on conflicts of competency among holders of legislative, executive and

- решава за судирот на надлежностите меѓу носителите на законодавната, извршната и судската власт; - решава за судирот на надлежностите меѓу прганите на Републиката и еденицте на локалната самоуправа; - одлучува за одговорноста на претседателот на Републиката; - одлучува за уставноста на програмите и статутите на политичките партии и на здруженијата н а граѓаните и - одлучува и за други прашања утврдени со Уставот.	judicial offices; - decides on conflicts of competency among Republic bodies and units of local self-government; - decides on the answerability of the President of the Republic; - decides on the constitutionality of the programmes and statutes of political parties and associations of citizens; and - decides on other issues determined by the Constitution.
Закон за медиуми Слобода на изразување и слобода на медиумите Член 3 (1) Се гарантира слободата на изразување и слободата на медиумите. (2) Слободата на медиумите особено опфаќа: слобода на изразување на мислења, независност на медиумите, слобода на прибирање, истражување, објавување, избор и пренесување на информации во насока на информирање на јавноста, плурализам и разновидност на медиумите, слобода на проток на информации и отвореност на медиумите за различни мислења, уверувања и за разновидни содржини, достапност до информациите од јавен карактер, почитување на човековата индивидуалност, приватност и достоинство, слобода за основање на правни лица за вршење на дејност за јавно информирање, печатење и дистрибуција на печатен медиум и другите медиуми од земјата и странство, производство и емитување на аудио/ аудиовизуелни програми, самостојност на уредникот, новинарот, авторите или креаторите на содржини или програмските	Law on media Freedom of expression and freedom of the media Article 3 (1) Freedom of expression and the freedom of the media are guaranteed. (2) Freedom of the media shall in particular cover: freedom of expression of opinion, independence of the media, freedom to gather, research, publish, select and disseminate information for the purpose of informing the public, pluralism and diversity of the media, freedom of information flow. and openness of the media to different opinions, beliefs and content, access to public information, respect for human individuality, privacy and dignity, freedom to establish legal entities to perform business for public information, printing and distribution of print media and other media from home and abroad, production and broadcasting of audio / Audiovisual programs, the autonomy of the editor, journalist, authors or content creators or programmers and other persons, in accordance with the rules of the profession. (3) The freedom of the media may be restricted only in accordance with the Constitution of the Republic of Macedonia

соработници и другите лица, а во согласност со правилата на професијата. (3) Слободата на медиумите може да биде ограничена само во согласност со Уставот на Република Македонија	
Закон за Медиуми Посебни забрани Член 4 (1) Забрането е со објавувањето, односно емитувањето на содржини во медиумите да се загрозува националната безбедност, да се поттикнува насилно уривање на уставниот поредок на Република Македонија, да се повикува на воена агресија или на вооружен конфликт, да се поттикнува или шири дискриминација, нетрпеливост или омраза врз основа на раса, пол, религија или националност. (2) Посебните забрани од ставот (1) на овој член треба да бидат во согласност со практиката на Европскиот суд за човекови права.	Law on Media Special prohibitions Article 4 (1) It is prohibited by the publication, that is, the broadcasting of contents in the media, to endanger national security, to encourage violent destruction of the constitutional order of the Republic of Macedonia, to invoke military aggression or armed conflict, to incite or spread discrimination; intolerance or hatred based on race, sex, religion or nationality. (2) The special injunctions referred to in paragraph (1) of this Article shall be in accordance with the practice of the European Court of Human Rights.
Право на исправка на објавена информација Член 17 (1) Секој има право од издавач на медиум, односно од одговорен уредник на издавач на медиум да бара, без надоместок, да објави исправка на објавена информација во која се наведуваат неточните факти објавени во информацијата, а со кои биле повредени неговите права или интереси. Право на исправка имаат и правните лица и други организации и тела, доколку со информацијата биле повредени нивните права или интереси. (2) Барањето за објавување на исправка се поднесува до одговорниот уредник на издавачот на медиум во писмена форма во рок од 30 дена од денот на објавувањето на информацијата на која се однесува исправката. Барањето мора да биде образложено и потпишано од страна на	Right to correct published information Article 17 (1) Everyone has the right to request from a media outlet or editor-in-chief for a media outlet to publish, without remuneration, a correction of published information indicating inaccurate facts disclosed in the information which infringed on his rights or interests. Legal persons and other organisations and bodies are also entitled to redress if their rights or interests are infringed by the information. (2) The request for publication of correction shall be submitted to the editor-in-chief of the media publisher in writing within 30 days from the date of publication of the information to which the correction applies. The request must be reasoned and signed by the correction submitter and contain all necessary data

подносителот на исправката и да ги содржи сите потребни податоци за подносителот на исправката, како и неговата адреса. (3) Во исправката на објавена информација покрај исправка на погрешните тврдења или неточните наводи во објавената информација, може да се изнесуваат факти и околности со кои подносителот на исправката ги побива или битно ги дополнува наводите во објавената информација. (4) Во случај кога се работи за научна или уметничка критика не се дава право на исправка, освен доколку со истата се врши само исправка на неточни факти. (5) Не може да се бара исправка доколку издавачот на медиум, до денот на поднесувањето на барањето за исправка, веќе претходно сам објавил исправка на истата информација. Ако подносителот на барањето за исправка смета дека издавачот на медиумот не ја објавил исправката на соодветен начин, во тој случај може да бара остварување на своето право во согласност со членот 23 од овој закон. (6) Доколку лицето за кое се однесува информацијата е починато, право на објавување на исправка имаат неговите деца, посвоени деца, брачните другари, родители, посвоители, браќа и сестри или правни лица, доколку информацијата се однесува на дејноста која ја вршело покојното лице во врска со тоа правно лице. (7) Подносителот на барањето за објавување на исправка мора јасно да ја наведе информацијата, односно податокот од информацијата на кој се однесува барањето за исправка и датумот на нејзината објава.	about the correction submitter as well as his address. (3) In correction of published information, in addition to correction of false claims or incorrect allegations in the published information, facts and circumstances may be set out by which the correction submitter refutes or substantially supplements the allegations in the published information. (4) In the case of scientific or artistic criticism, the right of correction is not granted, unless it corrects only the incorrect facts. (5) A correction may not be requested if the media publisher has already published a correction of the same information by the date of submission of the correction request. If the submitter of the request for correction considers that the publisher of the medium did not publish the correction in an appropriate manner, in that case, he may request the exercise of his right in accordance with Article 23 of this Law. (6) If the person to whom the information relates has died, his children, adopted children, spouses, parents, adoptive parents, brothers and sisters or legal persons shall have the right to make a correction if the information relates to the activity performed by the deceased person. in relation to that legal entity. (7) The person submitting the request for correction must clearly state the information, ie the information from the information to which the request for correction relates and the date of its publication.
Закон за медиуми Барање за исправка од издавач на медиум кој престанал да постои Член 22	Media Law Request for correction from a media publisher that has ceased to exist Article 22 (1) A correction may also be required when the information has been published

(1) Објава на исправка може да се бара и кога информацијата била објавена од издавач на медиум кој во меѓувреме престанал да постои. Подносителот на барањето за исправка има право од издавачот на тој медиум или од неговиот правен следбеник да бара, на негов трошок, да му обезбеди објавување на исправката во друг медиум кој по нивото на гледаност/слушаност, односно тираж е сличен со него.	by a media publisher which has in the meantime ceased to exist. The person submitting the correction request has the right to request from the publisher of that medium or his legal successor, at his own expense, to publish the correction in another medium which is similar to the level of viewership/listening or circulation.
Закон за медиуми Право на тужба Член 23 (1) Ако одговорниот уредник на издавач на медиум не ја објави исправката на начин и во роковите определени со членот 19 од овој закон, заинтересираното лице има право да покрене тужба против одговорниот уредник пред надлежниот суд во рок од 30 дена од истекот на рокот за објавување на исправката, односно од денот кога исправката не била објавена или била објавена на начин кој не е во согласност со овој закон. (2) Судските спорови во врска со објавата на исправката се решаваат по итна постапка. (3) Одговорниот уредник е должен при објавувањето на исправката по завршување на судската постапка да наведе дека објавувањето се извршува врз основа на правосилна судска пресуда и притоа е должен да ја цитира изречената пресуда.	Media Law Right to sue Article 23 (1) If the editor-in-chief of a media publisher fails to publish the correction in a manner and within the time limits specified in Article 19 of this Law, the interested person shall have the right to file a lawsuit against the editor-in-chief before the competent court within 30 days of the expiration of the deadline for publication of the correction, that is, from the day when the correction was not published or was published in a way that is not in accordance with this law. (2) The litigation regarding the announcement of the correction shall be resolved in urgent procedure. (3) The editor-in-chief shall be obliged when announcing the correction after the completion of the court procedure to state that the announcement is made on the basis of a final court verdict and is obliged to cite the pronounced verdict.
Закон за аудио и аудиовизуелни медиумски услуги Член 48 Посебни забрани (1) Аудио и аудиовизуелните медиумски услуги не смеат да содржат програми со кои се загрозува националната безбедност, се поттикнува насилно уривање на уставниот поредок на Република	Law on Audio and Audio-visual Media Services Article 48 Special prohibitions (1) Audio and audio-visual media services may not contain programs that endanger national security, incite violent destruction of the constitutional order of the Republic of Macedonia, invoke military aggression

Македонија, се повикува на воена агресија или на оружен конфликт, се поттикнува или шири дискриминација, нетрпеливост или омраза врз основа на раса, боја на кожа, потекло, национална или етничка припадност, пол, род, сексуална ориентација, родов идентитет, припадност на маргинализирана група, јазик, државјанство, социјално потекло, образование, религија или верско уверување, политичко уверување, друго уверување, попреченост, возраст, семејна или брачна состојба, имотен статус, здравствена состојба, лично својство и општествен статус, или која било друга основа. (2) Посебните забрани од ставот (1) на овој член треба да бидат во согласност со практиката на Европскиот суд за човекови права.	or armed conflict, incite or spread discrimination, intolerance or based on race, skin colour, origin, national or ethnic origin, gender, gender, sexual orientation, gender identity, belonging to a marginalised group, language, citizenship, social origin, education, religion or religion co beliefs, political convictions, other beliefs, disability, age, family or marital status, property status, health status, personal characteristics and social status, or any other basis. (2) The special injunctions referred to in paragraph (1) of this Article shall be in accordance with the practice of the European Court of Human Rights.
Закон за граѓанска одговорност за клевета и навреда Основни начела Член 2 (1) Законот ја гарантира слободата на изразување и информирање како една од битните основи на демократското општество. (2) Ограничувањата на слободата на изразување и информирање законски се уредуваат со определување на стриктни услови за граѓанска одговорност за навреда и клевета, во согласност со Европската конвенција за заштита на човековите права и основните слободи (член 10) и практиката на Европскиот суд за човекови права.	Law on Civil Liability for Defamation and Insult Basic principles Article 2 (1) The law guarantees freedom of expression and information as one of the essential foundations of a democratic society. (2) Restrictions on freedom of expression and information are legally regulated by stipulating strict conditions for civil liability for insult and defamation, in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 10) and the case law of the European Court of Human Rights.
Закон за граѓанска одговорност за клевета и навреда Одговорност за навреда Член 6	Law on Civil Liability for Defamation and Insult Responsibility for insult Article 6

(1) За навреда одговара тој што со намера да омаловажи, со изјава, однесување, објавување или на друг начин ќе изрази за друг понижувачко мислење, со кое се повредува неговата чест и углед.	(1) The person who deliberately humiliates, declares, behaves, publishes or otherwise expresses another humiliating opinion, which violates his honour and reputation, shall be liable for the offence.
(2) Одговорност за навреда постои и ако со такво дејствие се омаловажува угледот на правно лице, група лица или умрено лице.	(2) Liability for insult shall also exist if such act undermines the reputation of a legal person, group of persons or a deceased person.
(3) За навреда сторена преку средство за јавно информирање (весници, магазини и друг печат, програми на радиото и телевизијата, електронски публикации, телетекст и други форми на уреднички обликувани програмски содржини кои се објавуваат, односно се емитуваат дневно или периодично во пишана форма, звук или слика, на начин достапен за широката јавност), можат да одговараат авторот на изјавата, уредникот или лицето кое го заменува во средството за јавно информирање и правното лице. Тужителот при поднесувањето на тужбата е слободен да одлучи против кое од лицата од овој став ќе поднесе тужба за утврдување одговорност и надоместување на штета за навреда.	(3) For insult made through a mass media (newspapers, magazines and other press, radio and television programs, electronic publications, teletexts and other forms of editorially shaped program content that are published, i.e. broadcast daily or periodically in writing, sound or image, in a manner accessible to the general public), may be the responsibility of the author of the statement, the editor or the person replacing it in the media and the legal entity. The plaintiff is free to decide against which of the persons referred to in this paragraph to file a claim for liability and compensation for insult.
(4) Издавачот, уредникот или лицето што го заменува во средството за јавно информирање и правното лице кое го издава средството за јавно информирање, за навреда сторена од новинарот во тоа средство кој е автор на изјавата одговараат врз начелото на претпоставена одговорност.	(4) The publisher, the editor or the person replacing it in the media and the legal entity issuing the media shall, for the offence committed by the journalist in that medium who is the author of the statement, be held liable for the principle of presumed liability.
(5) Во случаите од ставовите 3 и 4 на овој член новинарот, како автор на изјавата, не одговара за навреда ако докаже дека објавувањето на навредливата изјава му било наложено од страна на уредникот или лицето кое го заменува, или содржината на неговата изјава е битно изменета од страна на уредникот или лицето кое го заменува.	(5) In the cases referred to in paragraphs 3 and 4 of this Article, the journalist, as the author of the statement, shall not be held liable for insult if he or she proves that the publication of the offensive statement was ordered by the editor or the person replacing it, or the content of his statement is significantly modified by the editor or the person replacing it.
(6)Новинарот како автор на изјавата не одговара ако таа добила навредлив карактер со нејзиното опремување со ставање на наслови, поднаслови, фотографии, извлекување на делови на изјавата од нејзината целовитост, најави	(6) A journalist as the author of a statement shall not be held liable if it has acquired an offensive character by equipping it by placing headlines, subheadings, photographs, extracting parts of the statement from its entirety, announcing or otherwise by the editor or the person replacing it.

или на друг начин од страна на уредникот или лицето кое го заменува.	
Закон за граѓанска одговорност за клевета и навреда Исклучување на одговорноста Член 7 (1) Нема одговорност за навреда, ако: 1) изјавата е дадена во работата на Собранието на Република Македонија, во работата на советите на општините и градот Скопје, во управна или судска постапка или пред Народниот правобранител, освен ако тужителот докаже дека е дадена злонамерно; 2) е пренесено мислење содржано во службен документ на Собранието на Република Македонија, Владата на Република Македонија, органите на управата, судовите или други државни органи, соопштение или други документи на меѓународни организации или конференции, соопштение или друг документ за информирање на јавноста издадени од надлежни државни органи, установи или други правни лица, соопштение или друг службен документ од истраги за сторени кривични дела или прекршоци и 3) во изјавата се пренесени мислења изнесени на јавен собир, во судска постапка или друга јавна манифестација на активноста на државни органи, установи, здруженија или правни лица или се известува за изјава што е јавно соопштена од друг. (2) Не е одговорен за навреда тој што во научно, книжевно или уметничко дело, во сериозна критика, во вршење на службена должност, новинарска професија, политичка или друга општествена дејност, во одбрана на слободата на јавно изразување на мислата или на други права или при заштита на јавен интерес или други оправдани интереси, ќе изнесе понижувачко мислење за друг, ако: 1) од начинот на изразувањето или од другите негови околности произлегува дека тоа нема значење на навреда; 2) не предизвикало значителна повреда на честа и угледот на личноста и 3) не е изнесено	Law on Civil Liability for Defamation and Insult Disclaimer Article 7 (1) There is no liability for insult if: 1) the statement is made in the work of the Assembly of the Republic of Macedonia, in the work of the councils of the municipalities and the City of Skopje, in administrative or judicial proceedings or before the Ombudsman, unless the plaintiff proves that it has been made malicious; 2) the opinion contained in an official document of the Assembly of the Republic of Macedonia, the Government of the Republic of Macedonia, the administrative authorities, the courts or other state authorities, a statement or other document issued to international organisations or conferences, a press release or other document issued by the public; competent state authorities, institutions or other legal entities, a statement or other official document from investigations into criminal offences or misdemeanours; and 3) the statement contains opinions expressed at a public meeting, in a judicial post. a petition or other public manifestation of the activity of state authorities, institutions, associations or legal entities or shall be notified of a statement made public by another. (2) The person who is not responsible for the insult in scientific, literary or artistic work, in serious criticism, in the performance of his official duty, journalistic profession, political or other social activity, in defence of the freedom of public expression of thought or other rights or, in the protection of the public interest or other justified interest, expresses a degrading opinion of another if: 1) the manner of expression or other circumstances proves that it has no meaning in the offence; 2) it has not

исклучиво со цел да се понижи личноста на друг или да се омаловажи неговата чест и углед. (3) Не е одговорен за навреда тој што ќе изнесе понижувачко мислење за носител на јавна функција во јавен интерес, ако докаже дека тоа е засновано врз вистинити факти, или ако докаже дека имал основана причина да поверува во вистинитоста на таквите факти, или ако изјавата содржи оправдана критика или поттикнува расправа од јавен интерес или е дадена во согласност со професионалните стандарди и етика на новинарската професија. (4) Не е одговорен за навреда тој што изнесува негативно мислење за друг со искрена намера или увереност во добронамерноста на неговото мислење. (5) При оценувањето на условите за исклучување на одговорноста судот ќе ги примени критериумите за оправдано ограничување на слободата на изразување содржани во Европската конвенција за заштита на човековите права и во судската практика на Европскиот суд за човекови права.	caused significant harm to the honour and reputation of the person, and 3) it has not been disclosed solely for the purpose of humiliating another's personality or degrading his honour and reputation. (3) A person who submits a humiliating opinion to a public office-holder in the public interest shall not be liable for the offence if he proves that it is based on factual facts, or if he proves that he had a well-founded reason to believe in the truth of such facts, or the statement contains justified criticism or incites debate in the public interest or is given in accordance with the professional standards and ethics of the journalistic profession. (4) A person who presents a negative opinion of another with a sincere intention or conviction in the good faith of his opinion shall not be liable for the insult. (5) In assessing the conditions for the exclusion of liability, the court shall apply the criteria for justifying a restriction on the freedom of expression contained in the European Convention for the Protection of Human Rights and in the case law of the European Court of Human Rights.
Закон за граѓанска одговорност за клевета и навреда Одговорност за клевета Член 8 (1) За клевета одговара тој што за друго лице со утврден или очевиден идентитет, со намера да наштети на неговата чест и углед, пред трето лице изнесува или пронесува невистинити факти што се штетни за неговата чест и углед, а знае или бил должен и може да знае дека се невистинити. (2) Одговорност за клевета постои и ако невистинитото тврдење содржи факти штетни за угледот на правно лице, група лица или умрено лице.	Law on Civil Liability for Defamation and Insult Liability for defamation Article 8 (1) A defamatory person shall be liable for any other person with an established or obvious identity, intending to harm his / her honour and reputation, in front of a third person, reports or transmits untrue facts that are detrimental to his / her honour and reputation, and knows or was obliged to do so, may know they are untrue. (2) Liability for defamation also exists if the false claim contains facts harmful to the reputation of a legal person, group of persons or a deceased person.

(3)Ако изнесувањето или пренесувањето невистинити тврдења за факти е сторено преку средство за јавно информирање (весници, магазини и друг печат, програми на радиото и телевизијата, електронски публикации, телетекст и други форми на уреднички обликувани програмски содржини кои се објавуваат, односно се емитуваат дневно или периодично во пишана форма, звук или слика, на начин достапен за широката јавност), за клевета можат да одговараат авторот на изјавата, уредникот или лицето кое го заменува во средството за јавно информирање и правното лице. Тужителот при поднесувањето на тужбата е слободен да одлучи против кое од лицата од овој став ќе поднесе тужба за утврдување одговорност и надоместување на штета за клевета. (4) Издавачот, уредникот или лицето кое го заменува во средството за јавно информирање и правното лице што го издава средството за јавно информирање, за клевета сторена од новинарот во тоа средство кој е автор на изјавата одговараат врз начелото на претпоставена одговорност. (5) Новинарот како автор на изјавата не одговара за клевета, ако докаже дека нејзиното објавување му е наложено од страна на издавачот, уредникот или лицето кое го заменува или содржината на неговата изјава е битно изменета од страна на уредникот или лицето кое го заменува. (6) Новинарот како автор на изјавата не одговара ако таа добила карактер на клевета со нејзиното опремување со ставање на наслови, поднаслови, фотографии, извлекување на делови од изјавата на нејзината целовитост, најави или на друг начин од страна на уредникот или лицето кое го заменува.	(3) If making or transmitting false allegations of fact has been done through a mass media (newspapers, magazines and other press, radio and television programs, electronic publications, teletexts and other forms of editorially shaped program content that are published, ie broadcast daily or periodically in written form, sound or image, in a manner accessible to the general public), the author of the statement, the editor or the person replacing him in the media and the legal entity may be liable for defamation. It is. The plaintiff is free to decide against which of the persons referred to in this paragraph to file a claim for damages and defamation. (4) The publisher, the editor or the person who replaces it in the media and the legal entity issuing the media, shall be liable for the defamation committed by the journalist in that media who is the author of the statement. (5) The journalist as the author of the statement shall not be liable for defamation if he proves that its publication has been ordered by the publisher, the editor or the person who replaces it or the content of his statement has been substantially modified by the editor or the person who replaces it. (6) The journalist as the author of the statement shall not be liable if she has acquired the character of defamation by equipping her by placing headlines, subheadings, photographs, extracting parts of her statement of completeness, announcements or otherwise by the editor or the acting-editor.
Закон за граѓанска одговорност за клевета и навреда Докажување на вистинитоста	Law on Civil Liability for Defamation and Insult Prove the truth

Член 9 (1) Тужениот е должен да ја докажува вистинитоста на фактите содржани во тврдењето. (2) Тужениот кој ќе ја докаже вистинитоста на своето тврдење или ќе докаже дека имал основана причина да поверува во неговата вистинитост нема да одговара за клевета. (3) По исклучок од ставовите 1 и 2 на овој член, товарот на докажување паѓа врз тужителот кој како носител на јавна функција има законска должност да даде објаснување за конкретни факти кои најнепосредно се поврзани или се од значење за вршењето на неговата функција, ако тужениот докаже дека имал основани причини за изнесување на тврдење што е од јавен интерес. (4) По исклучок од ставовите 1 и 2 на овој член, не е дозволено докажување на вистинитоста на факти кои се однесуваат на приватниот живот на тужителот, освен ако изнесувањето такви факти е сторено во научно, книжевно или уметничко дело, во сериозна критика, во вршење на службена должност, новинарска професија, политичка или друга општествена дејност, во одбрана на слободата на јавно изразување, на мислата или на други права или при заштита на јавен интерес. (5) Ако клеветата се состои во јавно префрлање на друг дека сторил кривично дело или дека е осуден за такво дело, одговорноста е исклучена ако изјавата е дадена во јавен интерес и ако лицето кое ја дало ќе ја докаже нејзината вистинитост или ќе докаже дека имал основана причина да поверува во вистинитоста на таквите факти.	Article 9 (1) The defendant shall be obliged to prove the truth of the facts contained in the allegation. (2) The defendant who will prove the truth of his claim or prove that he had a valid reason to believe in his truth shall not be liable for defamation. (3) By way of derogation from the paragraphs 1 and 2 of this Article, the burden of proof rests on the plaintiff who, as a public office holder, has a legal duty to provide an explanation of specific facts most directly related to or relevant to the performance of his or her function, if the defendant establishes that he had well-founded reasons for submitting a claim of public interest. (4) Notwithstanding paragraphs 1 and 2 of this Article, proof of the facts concerning the private life of the plaintiff shall not be allowed unless the disclosure of such facts has been committed in a scientific, literary or artistic work, in serious criticism, in the exercise of his official duty, journalistic profession, political or other social activity, in the defence of freedom of expression, of thought or other rights, or in the protection of the public interest. (5) If the defamation involves the public transfer of another to have committed a crime or is convicted of such an offence, liability shall be excluded if the statement is made in the public interest and if the person who gave it proves its truthfulness or proves that it had an established reason to believe in the truth of such facts.
Закон за граѓанска одговорност за клевета и навреда Одговорност на електронската публикација Член 11 (1) Уредникот на електронската публикација презема одговорност, заедно	Law on Civil Liability for Defamation and Insult Responsibility of the electronic publication Article 11 (1) The editor of the electronic publication shall be responsible, together with the

со авторот, за надоместување на штетата која произлегува од овозможување на пристап до навредливи или клеветнички информации. (2) Уредникот на електронската публикација не одговара за изнесена навреда или клевета како резултат на овозможување пристап до навредливи или клеветнички информации под услов доколку докаже дека: 1) авторот на информацијата објавена на електронската публикација не дејствувал под директна или индиректна контрола или влијание од страна на уредникот на електронската публикација и 2) не бил свесен ниту требал да биде свесен дека навредлив или клеветнички материјал е објавен на електронската публикација или во рок од 24 часа откако станал свесен за навредливиот и клеветнички карактер на објавениот текст или информација, ги презел сите технички и други мерки за отстранување на таквата информација. Барање за отстранување на информација може да поднесе и оштетеното лице.	author, for the compensation of the damage arising from the provision of access to offensive or defamatory information. (2) The editor of the electronic publication shall not be liable for any insult or defamation as a result of providing access to offensive or defamatory information provided he/she proves that: 1) the author of the information published in the electronic publication has not acted under direct or indirect control or influence by the editor of the electronic publication; and 2) was unaware or required to be aware that abusive or defamatory material was published in the electronic publication or within 24 hours after becoming aware As to the offensive and defamatory nature of the published text or information, it has taken all technical and other measures to remove such information. The injured party may also submit a request for removal of information.
Закон за граѓанска одговорност за клевета и навреда Член 23 (1) Со поднесувањето на тужба за утврдување на одговорност и надоместување на штетата, оштетениот може да поднесе до надлежниот суд барање за одредување на привремена судска мерка што се состои во забрана на натамошно објавување на навредливите или клеветничките изјави. (2) Барањето треба да содржи основи на верување кои упатуваат на навредливиот или клеветничкиот карактер на изјавата и нејзината штетност за честа и угледот на оштетениот. (3) Привремена мерка на забрана за натамошно објавување судот ќе донесе само ако е навредливата или клеветничката изјава веќе објавена и ако е основано	**Article 23** (1) Along with submitting the complaint about determination of liability and compensation for damage, the aggrieved party may submit a request for issuing a temporary court injunction banning any further publication of the insulting or defamatory statements to the competent court. (2) The request should include the grounds of belief which refer to the insulting or defamatory character of the statement and its harmfulness to the honour and reputation of the aggrieved party. (3) The court shall adopt a temporary injunction banning further publication only if the insulting or defamatory statement has been already published and if it has a grounded belief that its further publication shall cause irreparable non-

уверен дека со нејзиното натамошно објавување ќе биде предизвикана непоправлива нематеријална или материјална штета за оштетениот. (4) Судот ќе одлучи со решение за изрекување на привремена забрана во рок од три дена од доставувањето на барањето. Забраната се однесува само на конкретната навредлива или клеветничка изјава. (5) Судот ќе го одбие барањето од ставот (1) на овој член ако не содржи доволно основи на верување дека се однесува на навредлива или клеветничка изјава која е штетна за подносителот, или ако судот смета дека во конкретниот случај постојат основи за исклучување на одговорноста за навреда или клевета. Против решението подносителот на барањето има право на жалба до повисокиот суд во рок од три дена од неговото доставување.	material or material damage to the aggrieved party. (4) The court shall, by a decision, decide on ordering a temporary ban within a period of three days as of the submission of the request. The ban shall apply solely to the specific insulting or defamatory statement. (5) The court shall reject the request referred to in paragraph (1) of this Article if it does not contain enough grounds to believe that it refers to an insulting or defamatory statement which damages the plaintiff, or if the court deems that there are grounds for exemption from liability for insult or defamation in that specific case. The requesting entity shall have the right to file an appeal against the decision to the higher instance court within a period of three days as of its submission.
Закон за слободен пристап до информации од јавен карактер Предмет на законот Член 1 (1) Со овој закон се уредуваат условите, начинот и постапката за оставување на правото на слободен пристап до информации од јавен карактер со кои располагаат органите на државната власт и други органи и организации утврдени со закон, органите на општините, градот Скопје и општините во градот Скопје, установите и јавните служби, јавните претпријатија , правни и физички лица што вршат јавни овластувања утврдени со закон и дејности од јавен интереси политички партии во делот на приходите и расходите (во натамошниот текст: иматели на информации). (2) Правото за слободен пристап до информации од јавен карактер се остварува согласно овој, Законот за општата управна постапка и друг закон.	Law on Free Access to Public Information Subject of the law Article 1 (1) This Law shall regulate the conditions, manner and procedure for granting the right to free access to public information at the disposal of the state authorities and other restrictions and restrictions determined by law, the municipal authorities, the City of Skopje and the municipalities in the Republic of Macedonia. the City of Skopje, institutions and public services, public enterprises, legal entities and individuals carrying out public areas determined by law and activities of public interest to political parties in the area of revenue and expenditure (hereinafter: information holders)). (2) The right to free access to public information shall be exercised in accordance with this, the Law on General Administrative Procedure and other law.
Закон за слободен пристап до информации од јавен карактер	Law on Free Access to Public Information

Слободен пристап до информации Член 4 (1) Слободен пристап до информации имаат сите правни и физички лица. (2) Слободен пристап до информации имаат и странски правни и физички лица во согласност со овој и друг закон.	Free access to information Article 4 (1) All legal and natural persons have free access to information. (2) Foreign legal entities and natural persons shall also have free access to information in accordance with this and other laws.
Закон за слободен пристап до информации од јавен карактер Исклучок од слободен пристап до информации Член 6 (1) Имателите на информации можат да одбијат барање за пристап до: 1) информација која врз основа на закон претставува класифицирана информација со соодветен степен на класификација; 2) личен податок чие откривање би значело повреда на заштитата на личните податоци; 3) информација чие давање би значело повреда на доверливоста на даночната постапка; 4) информација стекната или составена за истрага, кривична или прекршочна постапка, за спроведување на управна и на граѓанска постапка, а чие давање би имало штетни последици за текот на постапката; 5) информација која ги загрозува правата од индустриска или интелектуална сопственост (патент, модел, мостра, стоковен и услужен жиг, ознака на потеклото на производот). (2) Информациите утврдени во ставот (1) на овој член, стануваат достапни кога ќе престанат причините за нивната недостапност. (3) По исклучок од ставот (1) на овој член имателите на информации ќе одобрат пристап до информација, по задолжително спроведениот тест на штетност со кој ќе се утврди дека со објавувањето на таквата информација последиците врз интересот кој се заштитува се помали од јавниот интерес утврден со закон што би се	Law on Free Access to Public Information Exception to free access to information Article 6 (1) The holders of information may refuse a request for access to: 1) information which by law constitutes classified information with an appropriate degree of classification; 2) personal data the disclosure of which would constitute a breach of personal data protection; 3) information the disclosure of which would violate the confidentiality of the tax procedure; 4) information obtained or compiled for investigation, criminal or misdemeanour proceedings, for the conduct of administrative and civil proceedings, the disclosure of which would have harmful consequences for the course of the procedure; 5) information that infringes industrial or intellectual property rights (patent, model, sample, trademark and service mark, the designation of origin of the product). (2) The information provided for in paragraph (1) of this Article shall become available when the reasons for their inaccessibility cease to exist. (3) Notwithstanding paragraph (1) of this Article, information holders shall grant access to information following a mandatory harm test to determine that the disclosure of such information has the effect on the protected interest less than the public interest, stipulated by law that would be achieved by the disclosure of information. (4) If the document or part thereof contains the information referred to in

постигнал со објавувањето на информацијата. (4) Ако документот или негов дел содржи информации од ставот (1) на овој член, што можат да се одвојат од документот без притоа да се загрози неговата безбедност, имателот на информации ги одвојува тие информации од документот и го известува барателот за содржината на останатиот дел од документот.	paragraph (1) of this Article, which may be separated from the document without jeopardising its security, the information holder shall separate that information from the document and notify the applicant of the contents of the document for the rest of the document.
Деловник на Уставниот суд на Република Северна Македонија Член 51 (1) Секој граѓанин што смета дека со поединечен акт или дејство му е повредено правото или слободата утврдени со членот 110 алинеја 3 од Уставот, може да бара заштита од Уставниот суд во рок од два месеца од денот на доставувањето на конечниот или правосилниот поединечен акт, односно од денот на дознавањето за преземање дејство со кое е сторена повредата, но не подоцна од 5 години од денот на неговото преземање.	Rules of Procedure of the Constitutional Court of the Republic of Northern Macedonia Article 51 (1) Any citizen who considers that an individual act or act has violated his or her right or freedom set forth in Article 110, indent 3 of the Constitution, it may seek protection by the Constitutional Court within two months of the date of the final or effective individual act. , that is, from the date of the finding of action to commit the infringement, but not later than 5 years after the date of its infringement.
Устав на Република Северна Македонија Член 16 Се гарантира слободата на уверувањето, совеста, мислата и јавното изразување на мислата. Се гарантира слободата на говорот, јавниот настап, јавното информирање и слободното основање на институции за јавно информирање. Се гарантира слободниот пристап кон информациите, слободата на примање и пренесување на информации. Се гарантира правото на одговор во средствата за јавно информирање. Се гарантира правото на исправка во средствата за јавно информирање. Се гарантира правото на заштита на изворот на информацијата во средствата за јавно информирање. Цензурата е забранета.	Constitution of the Republic of Northern Macedonia Article 16 The freedom of belief, conscience, thought and public expression of thought is guaranteed. Freedom of speech, public appearance, public information and the free establishment of public information institutions are guaranteed. Free access to information, freedom to receive and impart information is guaranteed. The right of reply in the mass media is guaranteed. The right of correction in the mass media is guaranteed. The right to protect the source of information in the mass media is guaranteed. Censorship is forbidden.

Законзаграѓанскаодговорностзанавреда и клевета: **Член 2** 1 Законотјагарантираслободатанаизразување и информирањекакоеднаодбитнитеосновина демократскотоопштество. 2 Ограничувањатанаслободатанаизразување и информирањезаконскисеуредуваатсоопределувањенастриктниусловизаграѓанскаодговорностзанавреда и клевета, восогласностсоЕвропскатаконвенцијазазаштитаначовековитеправа и основнитеслободи (член 10) и практикатанаЕвропскиотсудзачовековиправа.	Law on Civil Liability for Insult and Defamation: Article 2 1 The law guarantees freedom of expression and information as one of the essential foundations of a democratic society. 2 Restrictions on freedom of expression and information are legally regulated by the establishment of strict conditions for civil liability for insult and defamation, in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 10) and the practice of the European Court of Human Rights.
Законзаграѓанскаодговорностзанавреда и клевета: Член 3 Ако судот со примена на одредбите од овој закон не може да реши определено прашање поврзано со утврдувањето на одговорноста за навреда или клевета, или смета дека постои законска празнина или судир на одредбите на овој закон со Европската конвенција за заштита на основните човекови права, врз начелото на нејзино предимство над домашното право ќе ги примени одредбите на Европската конвенција за заштита на основните човекови права и становиштата на Европскиот суд за човекови права содржани во неговите пресуди.	Law on Civil Liability for Insult and Defamation: Article 3 If the court, by applying the provisions of this law, cannot resolve a particular issue related to the determination of liability for defamation or defamation, or considers that there is a legal gap or conflict with the provisions of this law with the European Convention for the Protection of Fundamental Human Rights, on the principle on its domestic law priority, it will apply the provisions of the European Convention for the Protection of Fundamental Human Rights and the positions of the European Court of Human Rights contained in its judgments.
Европска Конвенција за заштита начовековите права и основните слободи Член 10 Слобода на изразување 1. Секој човек има право на слобода на изразувањето. Ова право ги опфаќа слободата на мислење и слободата на примање и пренесување информации или	European Convention for the Protection of Human Rights and Fundamental Freedoms Article 10 Freedom of expression 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive

идеи, без мешање на јавната власт и без оглед на границите. Овој член не ги спречува државите, на претпријатијата за радио, филм и телевизија да им наметнуваат режим на дозволи за работа. 2. Остварувањето на овие слободи, коешто вклучува обврски и одговорности, може да биде под одредени формалности, услови, ограничувања и санкции предвидени со закон, кои во едно демократско општество претставуваат мерки неопходни за државната безбедност, територијалниот интегритет и јавната безбедност, заштитата на редот и спречувањето на нереди и злосторства, заштитата на здравјето или моралот, угледот или правата на другите, за спречување на ширењето на доверливи информации или за зачувување на авторитетот и непристрасноста на судството.	and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from imposing a work permit regime on radio, film and television undertakings. 2. The exercise of these freedoms, which includes duties and responsibilities, may be subject to certain formalities, conditions, restrictions and penalties provided for by law, which in a democratic society constitute measures necessary for state security, territorial integrity and public security, the protection of order. and the prevention of disorder and crime, the protection of the health or morals, the reputation or rights of others, to prevent the dissemination of confidential information or to preserve the authority and impartiality of the judiciary.
Кривичен Законик на Република Северна Македонија Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем Член 394-г Тој што преку компјутерски систем во јавноста шири расистички и ксенофобичен пишан материјал, слика или друга репрезентација на идеја или теорија која помага, промовира или поттикнува омраза, дискриминација или насилство, против кое било лице или група, врз основа на пол, раса, боја на кожа, род, припадност на маргинализирана група, етничка припадност, јазик, државјанство, социјално потекло, религија или верско уверување, други видови уверувања, образование, политичка припадност, личен или општествен статус, ментална или телесна попреченост, возраст, семејна или брачна состојба, имотен статус, здравствена состојба, или на која било друга основа предвидена со закон или со ратификуван меѓународен договор, ќе се казни со затвор од една до пет години.	Criminal code of North Macedonia Spreading racist and xenophobic material through a computer system Article 394-g (1): The person who through a computer system spreads resist and xenophobic written material, images or other representation of an idea or theory that assists, promotes or encourages hatred, discrimination or violence against any person or group based on their sex, race, skin colour, gender, membership in a marginalised group, ethnicity, language, citizenship, social origins, religion or religious persuasion, other types of persuasion, education, political affiliation, personal or social status, mental or physical disability, age, family or marital condition, property status, health condition or any other base envisaged with the law or ratifies international agreement, shall be punished with imprisonment of one to five years.

Европска Конвенција за заштита на човековите права Член 10, став 1: „Секој човек има право на слобода на изразувањето. Оваправо ги опфаќа слободата на мислење и слободата на примање и пренесување информации или идеи, без мешање на јавната власт и без оглед на границите. Овој член не ги спречува државите, на претпријатијата за радио, филм и телевизија..."	European Convention of Human Rights Article 10 (1) 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises…'
Европска Конвенција за заштита на човековите права Член 11, став 1: Секој човек има право на слобода на мирно собирањеи здружувањесодруги, вклучувајќиго и правотодаосновасиндикати и даимсепридружуванасиндикатитезазаштита насвоитеинтереси.	European Convention of Human Rights Article 11 (1): Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.
Европска Конвенција за заштита на човековите права Член 14 „...пол, раса, боја на кожата, јазик, вера, политичко или кое и да е друго мислење, национално или социјално потекло, припадност на национално малцинство, материјална положба, потекло по раѓање или кој и да е друг статус."	European Convention of Human Rights Article 14 '…sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.'
Кривичен законик на Северна Македонија Член 417, став 3: „Секој што шири идеи за супериорност на една трка над друга, или кој се залага за расна омраза, или поттикнува расна дискриминација, ќе му се изрече казна затвор од шест месеци до три години."	Criminal Code of North Macedonia Article 417, paragraph 3: 'Whosoever spreads ideas about the superiority of one race over another, or who advocates racial hate, or instigates racial discrimination, shall be sentenced to imprisonment of six months to three years.'
Кривичен законик на Северна Македонија Член 319, став 1: „Кој и да е со сила, малтретирајќи, загрозувајќи ја безбедноста, исмејувајќи го националниот, етничкиот, верскиот и други симболи, со палење, уништување или на кој било друг начин оштетување на знамето на Република	Criminal Code of North Macedonia Article 319, paragraph 1: 'Whosoever by force, maltreatment, endangering the security, mocking of the national, ethnic, religious and other symbols, by burning, destroying or in any other manner damaging the flag of the Republic of

Македонија или знамиња на други држави, со оштетување на туѓи предмети, со сквернавење на споменици, гробови или на кој било друг дискриминаторски начин, директно или индиректно, предизвикува или возбудува омраза, раздор или нетолеранција врз основа на пол, раса, боја на кожата, членство во маргинализирана група , етничко членство, јазик, националност, социјална позадина, религиозно убедување, други верувања, образование, политичка припадност, личен или социјален статус, ментално или физичко нарушување, возраст, семејство или брачен статус, статус на имот, здравствена состојба или во која било друга основа предвиден со закон за ратификуван меѓународен договор, ќе му се изрече казна затвор од една до пет години “. Став 2: „Кој го изврши кривичното дело од ставот (1) на овој член со злоупотреба на неговата позиција или овластување, или ако заради овие злосторства, против народот биле предизвикани немири и насилство, или била предизвикана штета во голема мерка ќе му се изрече казна затвор од една до десет години.“	Macedonia or flags of other states, by damaging other people's objects, by the desecration of monuments, graves, or in any other discriminatory manner, directly or indirectly, causes or excites hatred, discord or intolerance on grounds of gender, race, the colour of the skin, membership in marginalised group, ethnic membership, language, nationality, social background, religious belief, other beliefs, education, political affiliation, personal or social status, mental or physical impairment, age, family or marital status, property status, health condition, or in any other ground foreseen by law on ratified international agreement, shall be sentenced to imprisonment of one to five years.' Paragraph 2: 'Whosoever commits the crime referred to in paragraph (1) of this Article by abusing his position or authorisation, or if because of these crimes, riots and violence were caused against the people, or property damage to a great extent was caused, shall be sentenced to imprisonment of one to ten year.'
Кривичен законик на Северна Македонија Член 394-г „Кој и да е преку компјутерски систем се шири во јавниот расистички и ксенофобичен пишан материјал, фотографија или друга застапеност на идеја или теорија, помагајќи, промовирање или стимулирање на омраза, дискриминација или насилство, независно од тоа која личност или група, заснована на пол , раса, боја на кожа, класа, членство во маргинализирана група, етничка припадност, јазик, националност, социјална позадина, религиозно верување, други видови на верувања, образование, политичка припадност, лична или социјална состојба, ментална или физичка попреченост, возраст, семејство или брачниот статус, имотната состојба, здравствената состојба или која било друга основа предвидена со закон или ратификувана меѓународна спогодба, ќе се казни со затвор од една до пет години.“	Criminal Code of North Macedonia Article 394-d 'Whosoever via a computer system spreads in the public racist and xenophobic written material, photo or other representation of an idea or theory helping, promoting or stimulating hatred, discrimination or violence, regardless against which person or group, based on sex, race, skin colour, class, membership in a marginalised group, ethnic background, language, nationality, social background, religious belief, other types of beliefs, education, political affiliation, personal or social condition, mental or physical disability, age, family or marital status, property status, health condition, or any other ground foreseen by law or ratified international agreement, shall be sentenced to imprisonment of one to five years.'

Устав на Република Северна Македонија Член 16 Се гарантира слободата на уверувањето, совеста, мислата и јавното изразување на мислата. Се гарантира слободата на говорот, јавниот настап, јавното информирање и слободното основање на институции за јавно информирање. Се гарантира слободниот пристап кон информациите, слободата на примање и пренесување на информации. Се гарантира правото на одговор во средствата за јавно информирање. Се гарантира правото на исправка во средствата за јавно информирање. Се гарантира правото на заштита на изворот на информацијата во средствата за јавно информирање. Цензурата е забранета.	Constitution of the Republic of North Macedonia Article 16 The freedom of belief, conscience, thought and public expression of thought is guaranteed. Freedom of speech, public appearance, public information and the free establishment of public information institutions are guaranteed. Free access to information, freedom to receive and impart information is guaranteed. The right of reply in the mass media is guaranteed. The right of correction in the mass media is guaranteed. The right to protect the source of information in the mass media is guaranteed. Censorship is forbidden.
Закон за заштита на лични податоци Член 2 Одделни изрази употребени во овој закон го имаат следново значење: 1. “Личен податок” е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува, а лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, ментален, економски, културен или социјален идентитет; 2. „Обработка на личните податоци" е секоја операција или збир на операции што се изведуваат врз лични податоци на автоматски или друг начин, како што е: собирање, евидентирање, организирање, чување, приспособување или промена, повлекување, консултирање, употреба,откривање преку пренесување,	Law on Personal Data Protection Article 2 Certain terms used in this Law shall have the following meaning: 1. “ Personal data “ means any information relating to an identified natural or identifiable natural person, and a person who can be identified is a person whose identity can be ascertained directly or indirectly, specifically on the basis of citizen’s identification number or based on one or more features specific to his / her physical, physiological, mental, economic, cultural or social identity; 2. ‘personal data processing’ shall mean any operation or set of operations performed on personal data in an automated or other manner, such as collecting, recording, organising, storing, adapting or modifying, retracting, consulting, using, disclosing by transferring, posting or otherwise making available, equalising, combining, blocking, deleting or destroying;

објавување или на друг начин правење достапни, изедначување, комбинирање, блокирање, бришење или уништување; 3. „Збирка на лични податоци" е структурирана група лични податоци која е достапна согласно со специфични критериуми, без оглед дали е централизирана, децентрализирана или распространета на функционална или географска основа. 4. „Субјект на лични податоци" е секое физичко лице на кое се однесуваат обработените податоци; 5. „Контролор на збирка на лични податоци" е физичко или правно лице, орган на државната власт или друго тело, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци (во натамошниот текст: контролор). Кога целите и начинот на обработка на личните податоци се утврдени со закон или друг пропис, со истиот закон, односно пропис се определуваат контролорот или посебните критериуми за негово определување; 6. „Обработувач на збирка на лични податоци" е физичко или правно лице или законски овластен орган на државната власт кое ги обработува личните податоци за сметка на контролорот; 7. „Трето лице" е секое физичко или правно лице, орган на државната власт или друго тело, кое не е субјект на лични податоци, контролор, обработувач на збирка на лични податоци или лице кое под директно овластување на контролорот или обработувачот на збирка на лични податоци е овластено да ги обработува податоците; 8. „Корисник" е физичко или правно лице, орган на државната власт или друго тело на кое му се откриваат податоците. Органите на кои можат да им се откриваат податоците во рамките на посебна истрага, не се сметаат за корисници во смисла на овој закон; 9. „Согласност на субјектот на лични податоци" е слободно и изречно дадена	3. 'Collection of personal data' means a structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or disseminated on a functional or geographical basis. 4. 'personal data subject' shall mean any natural person to whom the processed data relate; 5. 'Controller of personal data collection' shall mean a natural or legal person, a body of state authority or other body, which independently or together with others determines the purposes and manner of processing personal data (hereinafter: controller). When the purposes and the manner of processing of personal data are determined by law or other regulation, the same law or regulation shall specify the controller or the specific criteria for its determination; 6. 'personal data collection processor' shall mean a natural or legal person or a legally authorised body of the state authority that processes personal data for the account of the controller; 7. 'Third party' shall mean any natural or legal person, public authority or other body not a personal data subject, a controller, a personal data processor or a person who is under the direct authority of the controller or processor of the personal data collection. personal data is authorised to process the data; 8. 'Beneficiary' shall mean a natural or legal person, a body of public authority or other body to whom the data are disclosed. ; 9. 'Consent of the personal data subject' shall mean a free and explicit statement of the will of the personal data subject with which he/she agrees to the processing of his / her personal data for predetermined purposes; 10. 'Specific categories of personal data' shall mean personal data revealing racial or ethnic origin, political, religious, philosophical or other beliefs, membership in trade unions and data

изјава на волја на субјектот на лични податоци со која се согласува со обработката на неговите лични податоци за однапред определени цели; 10. „Посебни категории на лични податоци" се лични податоци кои го откриваат расното или етничко потекло, политичко, верско, филозофско или друго уверување, членството во синдикална организација и податоци што се однесуваат на здравјето на луѓето, вклучувајќи ги и генетските податоци, биометриски податоци или податоци кои се однесуваат на сексуалниот живот; 11. „Трета земја“ е земја која не е членка на Европската унија или не е членка на Европскиот економски простор.	relating to human health, including genetic data, biometric data or data relating to sex life; 11. 'Third country' means a country which is not a member of the European Union or is not a member of the European Economic Area.
Закон за заштита на лични податоци Член 3-а Заштитата на личните податоци се гарантира на секое физичко лице без дискриминација заснована врз неговата националност, раса, боја на кожата, верски уверувања, етничка припадност, пол, јазик, политички или други верувања, материјална положба, потекло по раѓање, образование, социјално потекло, државјанство, место или вид на престој или кои било други лични карактеристики.	Law on Personal Data Protection Article 3-a The protection of personal data is guaranteed to any individual without discrimination based on his / her nationality, race, skin colour, religious beliefs, ethnicity, sex, language, political or other beliefs, material standing, ancestry, education, social origin, citizenship, place or type of residence or any other personal characteristics.
Закон за граѓанска одговорност за навреда и клевета Во членот 6 се вели дека „сторителот е одговорен за навреда, клевета, клевета или на друг начин искажува туѓо понижувачко мислење, што ја нарушува неговата чест и углед. Одговорност за навреда постои и ако таквиот чин го нарушува угледот на правно лице, група на лица или починато лице.“	Law on Civil Liability for Insult and Defamation Article 6 states that 'The offender is liable for insulting, defamatory, defamatory, or otherwise expressing another's humiliating opinion, which violates his honour and reputation. Liability for insult also exists if such act degrades the reputation of a legal person, group of persons or a deceased person.'
Закон за граѓанска одговорност за навреда и клевета Член 8 1 За клевета одговара тој што за друго лице со утврден или очевиден идентитет, со намера да наштети на неговата чест и	Law on Civil Liability for Insult and Defamation Article 8 1 It is liable for defamation that for another person with a determined or obvious identity, with the intent to harm

углед, пред трето лице изнесува или пронесува невистинити факти што се штетни за неговата чест и углед, а знае или бил должен и може да знае дека се невистинити	his honour and reputation, in front of a third person presents or transmits untrue facts that are detrimental to his honour and reputation and knows or is obliged and may know they are untrue
2 Одговорност за клевета постои и ако невистинитото тврдење содржи факти штетни за угледот на правно лице, група лица или умрено лице.	2 Liability for defamation exists even if the false claim contains facts harmful to the reputation of a legal person, group of persons or a deceased person.
3 Ако изнесувањето или пронесувањето невистинити тврдења за факти е сторено преку средство за јавно информирање (весници, магазини и друг печат, програми на радиото и телевизијата, електронски публикации, телетекст и други форми на уреднички обликувани програмски содржини кои се објавуваат, односно се емитуваат дневно или периодично во пишана форма, звук или слика, на начин достапен за широката јавност), за клевета можат да одговараат авторот на изјавата, уредникот или лицето кое го заменува во средството за јавно информирање и правното лице. Тужителот при поднесувањето на тужбата е слободен да одлучи против кое од лицата од овој став ќе поднесе тужба за утврдување одговорност и надоместување на штета за клевета.	3 If making or transmitting false allegations of fact is done through a mass media (newspapers, magazines and other press, radio and television programs, electronic publications, teletexts and other forms of editorially shaped program content that are published or broadcast daily or periodically in writing, sound or image, in a manner accessible to the general public), the defamation may be claimed by the author of the statement, the editor or the person replacing it in the media and the legal entity is. The plaintiff is free to decide against which of the persons referred to in this paragraph to file a claim for damages and defamation.
4 Издавачот, уредникот или лицето кое го заменува во средството за јавно информирање и правното лице што го издава средството за јавно информирање, за клевета сторена од новинарот во тоа средство кој е автор на изјавата одговараат врз начелото на претпоставена одговорност.	4 The publisher, the editor or the person replacing it in the media and the legal entity issuing the media, for defamation committed by the journalist in that medium who is the author of the statement, are held liable for the principle of presumed liability.
5 Новинарот како автор на изјавата не одговара за клевета, ако докаже дека нејзиното објавување му е наложено од страна на издавачот, уредникот или лицето кое го заменува или содржината на неговата изјава е битно изменета од страна на уредникот или лицето кое го заменува.	5 A journalist as the author of a statement shall not be held liable for defamation if he proves that its publication has been ordered by the publisher, the editor or the person who replaces it or the content of its statement has been substantially modified by the editor or the person replacing it.
6 Новинарот како автор на изјавата не одговара ако таа добила карактер на клевета со нејзиното опремување со ставање на наслови, поднаслови, фотографии, извлекување на делови од изјавата на нејзината целовитост, најави	6 A journalist as the author of a statement is not liable if she has acquired the character of defamation by equipping her with captions, subheadings, photographs, extracting parts of her statement of completeness, announced or otherwise by the editor or the person replacing her.

или на друг начин од страна на уредникот или лицето кое го заменува.	
Закон за граѓанска одговорност за навреда и клевета Член 19 1. Постапката се поведува со тужба за утврдување на одговорност и надоместување на штета за навреда или клевета, поднесена од оштетеното физичко или правно лице или неговиот законски застапник или старател. 2. Ако е оштетениот дете, овластен за поднесување тужба е неговиот родител или старател. 3. Ако е навредата или клеветата сторена спрема умрено лице, овластени за поднесување тужба се неговиот брачен другар, децата, родителите, браќата или сестрите, посвоителот, посвоеникот или друго лице со кое умреното лице живеело во заедничко домаќинство, ако со навредата или клеветата е нанесена штета на нивната чест и углед. 4. Лице кое врши јавна функција, оштетено со навреда или клевета, може да се појави како тужител само во неговото лично својство на физичко лице.	Law on Civil Liability for Insult and Defamation Article 19 1. The proceedings are instituted by a lawsuit establishing the responsibility and compensation for defamation or defamation brought by the injured natural or legal person or his or her legal representative or guardian. 2. If the injured child is a parent or guardian authorised to file a claim. 3. If the offence or defamation is committed against a deceased person, the spouse, children, parents, brothers or sisters, the adoptive parent, the adoptive parent or other person with whom the deceased person lived in a joint household are entitled to file a lawsuit if the offence or defamation has been inflicted damage to their honour and reputation. 4. A public official damaged, defamed or defamed may appear as a plaintiff only in his or her personal capacity as a natural person.
Закон за граѓанска одговорност за навреда и клевета Член 20 1. Рокот за поднесување на тужба според одредбите на овој закон е три месеци од денот кога тужителот дознал или требало да дознае за навредливата или клеветничката изјава и за идентитетот на лицето кое ја предизвикало штетата, но не подоцна од една година од денот кога изјавата е дадена пред трето лица. 2. Ако тужителот умре по започнувањето, но пред завршувањето на постапката со правосилна одлука, неговиот наследник може да ја продолжи постапката во име на умрениот, ако поднесе барање за продолжување на постапката најдоцна во рок од три месеци од смртта на тужителот.	Law on Civil Liability for Insult and Defamation Article 20 1. The time limit for filing a lawsuit under the provisions of this Act shall be three months from the date on which the plaintiff learned or should have known of the offensive or defamatory statement and of the identity of the person causing the damage, but no later than one year after the statement was made. given to third parties. 2. If the plaintiff dies after the commencement, but before the end of the proceedings by a final decision, his successor may continue the proceedings on behalf of the deceased, if he files a request for a continuation of the

	proceedings within three months of the plaintiff's death at the latest.
Закон за граѓанска одговорност за навреда и клевета Член 23 1. Со поднесувањето на тужба за утврдување на одговорност и надоместување на штетата, оштетениот може да поднесе до надлежниот суд барање за одредување на привремена судска мерка што се состои во забрана на натамошно објавување на навредливите или клеветничките изјави. 2. Барањето треба да содржи основи на верување кои упатуваат на навредливиот или клеветничкиот карактер на изјавата и нејзината штетност за честа и угледот на оштетениот. 3. Привремена мерка на забрана за натамошно објавување судот ќе донесе само ако е навредливата или клеветничката изјава веќе објавена и ако е основано уверен дека со нејзиното натамошно објавување ќе биде предизвикана непоправлива нематеријална или материјална штета за оштетениот. 4. Судот ќе одлучи со решение за изрекување на привремена забрана во рок од три дена од доставувањето на барањето. Забраната се однесува само на конкретната навредлива или клеветничка изјава. 5. Судот ќе го одбие барањето од ставот 1 на овој член ако не содржи доволно основи на верување дека се однесува на навредлива или клеветничка изјава која е штетна за подносителот, или ако судот смета дека во конкретниот случај постојат основи за исклучување на одговорноста за навреда или клевета. Против решението подносителот на барањето има право на жалба до повисокиот суд во рок од три дена од неговото доставување.	Law on Civil Liability for Insult and Defamation Article 23 1. By filing a claim for liability and damages, the aggrieved party may file with the competent court a request for a provisional injunction prohibiting the further publication of the offensive or defamatory statements. 2. The request shall contain grounds of belief indicating the offensive or defamatory nature of the statement and its harm to the honour and reputation of the injured party. 3. A provisional injunction prohibiting further disclosure shall be rendered by the court only if the defamatory or defamatory statement has already been published and if it is reasonably convinced that its further publication will cause irreparable non-pecuniary or non-pecuniary damage to the injured party. 4. The court shall decide on a temporary injunction within three days of the service of the request. The prohibition applies only to the specific offensive or defamatory statement. 5. The court shall reject the request referred to in paragraph 1 of this Article if it does not contain sufficient grounds to believe that the offending or defamatory statement is detrimental to the applicant, or if the court considers that in the present case there are grounds for excluding the liability for insult. or defamation. The claimant has the right to appeal to the higher court against the decision within three days of its submission.

Bibliography

English titles

Legislation

Constitution of the Republic of North Macedonia ('Official Gazette of the RNM' no.52/1991).

Law on Media ('Official Gazette of the RNM' no.184/2013 and 13/2014).

Law on Audio and Audiovisual Media Services ('Official Gazette of the RNM', no. 184/2013, 13/2014, 44/2014, 101/2014, 132/2014, 142/2016, 132/2017, 168/2018, 248/2018 and 27/2019).

Law on Civil Liability for Insult and Defamation ('Official Gazette of the RNM' no.143/2012).

Criminal Code ('Official Gazette of the RNM' nos. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 and 248/2018). Decisions of the Constitutional Court of the RNM: U. no. 220/2000 dated 30 May 2001, published in the 'Official Gazette of the RNM' no. 48/2001; U. no. 210/2001 dated 06 February 2002, published in the 'Official Gazette of the RNM' no. 16/2002; U. no. 206/2003 dated 09 June 2004, published in the 'Official Gazette of the RNM' no. 40/2004; U. no. 228/2005 dated 05 April 2004, published in the 'Official Gazette of the RNM' no. 50/2006; and U. no. 169/2016 dated 16 November 2017, published in the 'Official Gazette of the RNM' no. 170/2017.

Law on Classified Information ('Official Gazette of the RNM' no.257/19).

Law on Free Access to Public Information ('Official Gazette of the RNM' no.101/19).

Rules of Procedure of the Constitutional Court of the Republic of North Macedonia ('Official Gazette of the RNM' no.70/92 and 202/19).

Council of Europe, European Convention on Human Rights, as amended by Protocols Nos. 11 and 14, 4 November1950, ETS 5, available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf, ratified 10 April 1997. [accessed 10 February 2020].

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217, A (III), available at: https://www.un.org/en/universal-declaration-human-rights.[accessed 10 February 2020].

UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, page 171, available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, ratified 1994.[accessed 10 February 2020].

Law on the ratification of Statute of Council of Europe, Official Gazette of the Republic of Macedonia no 53/1995 of 08.11.1995

Law on amending and supplementing the law on media, Official Gazette of the Republic of Macedonia no 13/2014 of 23.01.2014

Law on the legal personality of churches, belief communities and religious groups, Official Gazette of the Republic of Macedonia no 113/2007 of 20.09.2007

Law on prevention and protection against discrimination, Official Gazette of the Republic of North Macedonia no 101/2019 of 22.05.2019

Law on public assembly, Official Gazette of the Republic of Macedonia no 55/1995 of 13.11.1995

Criminal Code, Official Gazette of the Republic of Macedonia no 37/1996 of 29.07.1996

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5

Reports

Council of Europe, Guide to good and promising practices on the way of reconciling freedom of expression with other rights and freedoms, in particular in culturally diverse societies (Steering Committee on Human Rights (CDDH), Council of Europe, 2019)

Study on the Media Regulatory framework and the online media – The Macedonian case, Comparative analysis and recommendations as to possible amendments to the legal framework

Digital resources

https://promedia.mk/main

Macedonian titles

Legislation

Устав на Република Северна Македонија („Службен весник на РСМ“ бр.52/1995).

Закон за медиуми („Службен весник на РСМ“ бр.184/2013 и 13/2014)

Закон за аудио и аудиовизуелни медиумски услуги („Службен весник на РСМ“ бр.184/2013, 13/2014, 44/2014, 101/2014, 132/2014, 142/2016, 132/2017, 168/2018, 248/2018 и 27/2019).

Закон за граѓанска оговорност за клевета и навреда („Службен весник на РСМ“ бр.143/2012).

Кривичен законик (Службен весник на РСМ“ бр.37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017 and 248/2018). Одлуки на Уставниот суд на Република Македонија: У. бр. 220/2000 од 30 мај 2001 година, објавена во „Службен весник на Република Македонија“ бр. 48/2001; У. бр. 210/2001 од 6 февруари 2002 година, објавена во „Службен весник на Република Македонија“ бр. 16/2002; У. бр. 206/2003 од 9 јуни 2004 година, објавена во „Службен весник на Република Македонија“ бр. 40/2004; У. бр. 228/2005 од 5 април 2006 година, објавена во „Службен весник на Република Македонија“ бр. 50/2006 и У. бр. 169/2016 од 16 ноември 2017 година, објавена во „Службен весник на Република Македонија“ бр. 170/2017.

Закон за класифицирани информации („Службен весник на РСМ“ бр.257/19).

Закон за слободен пристап до информации од јавен карактер („Службен весник на РСМ“ бр.101/19).

Деловник на Уставниот суд на Република Северна Македонија („Служен весник на РСМ“ бр.70/92 и 202/19).

СоветнаЕвропа,ЕвропскаКонвенцијазачовековиправа, изменетасоПротоколитебр. 11 и 14 ноември 1950 година, ETC 5, достапнана: https://www.echr.coe.int/Document/Convention_ENG.pdf,ратификувана 10 април 1997 година. [пристапенона: 10 февруари 2020 година].

Генералнотособраниена ООН, Универзалнадекларацијазачовековиправа, 10 декември 1948 година, 217, A (III), достапнона: https://www.un.org/en/universal-declaration-human-rights .[пристапенона: 10 февруари 2020 година].

Генералнотособраниена ООН, Меѓународенпактзаграѓански и политичкиправа, 16 декември 1966 година, Обединетитенации, Договориодсерија, том. 999, стр. 171, достапнона: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx ,ратификуван 1994 година. [пристапенона: 10 февруари 2020 година].

Закон за ратификација на Статутот на Советот на Европа, Службен Весник на Република Македонија бр 53/1995 од 08.11.1995

Законзаизменување и дополнувањеназаконотзамедиуми, Службен Весник на Република Македонија бр 13/2014 од 23.01.2014

Законзаправнатаположбанацрква, версказаедница и религиознагрупа, Службен Весник на Република Македонија бр 113/2007 од 20.09.2007

Законзаспречување и заштитаоддискриминација, Службен Весник на Република Северна Македонија бр 101/2019 од 22.05.2019

Законзајавнитесобири, Службен Весник на Република Македонија бр 55/1995 од 13.11.1995

Reports

Совет на Европа, Водичзадобри и

ветувачкипрактикизаначинотнаусогласувањенаслободатанаизразувањесодругиправа ислободи, особеновокултурноразновиднитеопштества (Управниоткомитетзачовековиправа (ЦДДХ), СоветнаЕвропа, 2019 година)

Годишен извештај за 2018 година за говор на омраза од Хелсиншкиот комитет за човекови права, Хелсиншки комитет, 2019

Слобода на Интернет во Северна Македонија, Метаморфозис, 2017

ELSA Poland

Contributors

National Coordinator

Bernadetta Semczuk

National Researchers

Agnieszka Fortuna

Paweł Jędrysiak

Aleksandra Kubińska

Adrianna Pasterska

Natalia Rogólska

Emilia Staniak

National Linguistic Editor

Marta Gruszka

National Technical Editor

Agnieszka Fortuna

National Academic Supervisor

dr hab. Katarzyna Grzybczyk,

professor of the University of Silesia in Katowice

Introduction

In the 21st century, the Internet has become an inherent element of our lives. Many various discussions take place in social media every day. Even though most of us do not really see the difference between a spoken word and a written one, it does exist and often causes problems from a legal point of view.

The primary concern of this research is to find out how do we strike a balance between safeguarding and surveillance. In this report authors tried to answer many questions that had arisen over recent years, that is what are the legal solutions existing in Polish law concerning freedom of expression online, protection of privacy, IP-rights and legitimacy of information and what else can the legislator do to make those regulations even more effective.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

1.1. Freedom of expression

Freedom of expression includes all verbal or non-verbal expression, thoughts or beliefs. Often, freedom of expression is understood as freedom to express which means the ability to convey ideas or information in any form and to selected recipients[1673]. Due to the development of mass media, freedom of expression over time adapts new manifestations of human activity. It may be exercised by i.a. press, television, radio, internet network, etc.

As a part of freedom of expression, we can distinguish the freedom of speech, which is defined as 'the right to freely express one's thoughts'[1674]. The right to the freedom of speech is directly protected by the highest legal act in Poland – the Constitution of the Republic of Poland of 2 April 1997, hereinafter referred to as the: 'Constitution'[1675]. Its Article 54 states that: "1. The freedom to express opinions, to acquire and to disseminate information shall be guaranteed to everyone. 2. Preventive censorship of the means of social communication and the licensing of the press shall be prohibited. Statutes may require obtaining a permit for the operation of a radio or television station'. This regulation

[1673] J. Sobczak, Swoboda wypowiedzi w orzecznictwie Trybunału Praw Człowieka w Strasburgu. Cz. 1 (Freedom of Expression in case law of the Court of Human Rights. Part 1), 'Ius Novum' 2007, no 2-3, page 5.

[1674] Under address: <https://sjp.pwn.pl/sjp/wolnosc-slowa;2537413.html> [access: 28/01/2020].

[1675] Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997 no. 78 pos. 483 as amended).

guarantees three separate rights, which are interrelated: freedom of expression, freedom of obtaining information and freedom of dissemination of information.

It should be noted that the notion of 'opinion' indicated in Article 54 sec. 1 of the Constitution is understood very broadly. It can mean presenting your own opinions, expressing assessments, informing about facts. The right to freedom of expression applies both at private and public levels and includes both natural persons and legal entities. The understanding of 'expressing views' also goes beyond just verbal statements[1676].

Freedom of expression includes freedom 'from' and freedom 'to'. Freedom 'from' is understood as the absence of state interference in the sphere of individual freedom expressed both in active and passive form (right to silence). In contrast, freedom 'to' is the activity of the state which creates the environment in which an individual can exercise his freedom. Its special example is the right to information[1677].

Rights and freedoms can be arranged in a hierarchy, they are valued and subordinated to other rights and freedoms, in particular those recognised as fundamental. Rights and freedoms are also limited when they come into contact with the rights and freedoms of others. Their implementation may not infringe or restrict the rights and freedoms of others. The universal principle is that one person's freedom ends where the other person's freedom begins[1678].

Freedom of expression is of great importance for the functioning of a democratic state ruled by law, the existence of which is assumed in Article 2 of the Constitution: 'The Republic of Poland shall be a democratic state ruled by law and implementing the principles of social justice'. This freedom allows citizens to obtain information necessary for participation in public life and democratic governance. It also aims to control state and local authorities, and thus to eliminate corruption and arbitrariness. It has a positive effect on relations between the rulers and the ruled[1679].

1676 Retrieved from URL: <https://www.rpo.gov.pl/pl/kategoria-konstytucyjna/art-54-wolnosc-slowa> [access: 28/01/2020].

1677 J. Mrozek, Rozważania prawne wokół pojęcia 'wolność słowa'(Legal considerations around the concept of 'freedom of speech'), Retrieved from URL: <http://uwm.edu.pl/mkks/wp-content/uploads/11-cz-4-mrozek.pdf> [access: 04/02/2020]

1678 J. Szymanek, Konstytucyjna zasada wolności słowa w radiofonii i telewizji (Constitutional principle of freedom of speech in radio and television), 'Państwo I Prawo'('State and Law') 2007, no. 8, page 18

1679 A. Wiśniewski, Znaczenie wolności słowa w państwie demokratycznym (The importance of freedom of speech in a democratic state), 'Gdańskie Studia Prawnicze' ('Legal Studies of Gdansk') 2000, no 7, page 650.

One of the manifestations of freedom of expression is freedom of the press, designed to provide citizens with access to reliable information. Freedom of the press is qualified as political freedom, which means that it is not absolute and there are circumstances in which it should be restricted. Freedom of media is now closely related to freedom of the press.

1.2. Censorship

The Constitution of the Republic of Poland provides for that there are situations in which freedom of expression may be restricted. Under Article 31 Section 3 of the Constitution: 'Any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights'. When introducing such restrictions, it becomes necessary to answer several questions, examples of which are provided by the Constitutional Tribunal:

- Will the introduced legislative regulation lead to its intended effects?

- Is this regulation necessary to protect the public interest associated?

- Will the effects of the introduced regulation remain in proportion to the burdens it imposes on the citizen?[1680]

There are no specific acts in polish law that introduce the regulation of internet censorship.

1.3. Right to Information

The Right to Information is directly expressed in Article 61 of the Constitution: '1. A citizen has the right to obtain information on the activities of the organs of public authority as well as persons exercising public functions. Such rights include obtaining the information on the activities of local government's bodies - economic or professional organs and other persons or organisational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury. 2. The right to obtain information ensures access to documents and entry to sittings of collective organs of public authority formed by universal elections, with the opportunity to make sound and visual recordings. 3. Limitations upon the rights referred to

[1680] Retrieved from URL:
<https://radcakancelaria.pl/2012/01/26/wolnosc-slowa-kilka-uwag-prawnych/>
[access: 07/02/2020].

in sections 1 and 2 above, may be imposed by the statute solely to protect freedoms and rights of other persons and economic subjects, public order, security or important economic interests of the State. 4. The procedure of providing the information referred to in sections 1 and 2 above are specified by the statute, and regarding the Sejm and the Senate by their regulations'.

A special law regulating the right to information in Poland is the Act of 6 September 2001 on access to public information[1681]. Article 1 of this Act provides that any information regarding public matters constitutes public information. Everyone has access to this information without having to prove a legal or factual interest. Article 3 of the abovementioned Act specifies that this right in question includes the right to obtain processed or unprocessed information, to view official documents or to access meetings of collegiate public authorities coming from the general election. The right to public information is also subject to restrictions enumerated in the Act. Among them is the privacy of a natural person (except for persons performing public functions, if the information is related to the performance of this function) or the secret of the entrepreneur. In principle, the information should be made available through the Public Information Bulletin or the central repository. In the absence of such disclosure, the information shall be made available on request. The request must be made in writing if the information cannot be/made available promptly.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

Poland is one of the EU Member States that do not have one specific legislation on blocking and taking down content on the internet. The absence of a general act, that would be a framework coordinating specific regulations, results in numerous rules scattered across many different acts. This legal matter requires a holistic approach and knowledge from different branches of law to fully understand its scope.

2.1. Blocking internet content related to terrorism

Nowadays, when the use of the internet is widespread, the benefits of technical progress are not always used with good intentions. When it comes to blocking the internet content, one of the most significant regulations is blocking the

[1681] Act of 6 September 2001 on access to public information (Journal of Laws of 2019, item 1429, uniform text).

accessibility of data related to a terrorist crime in the Information and Communications Technology (hereinafter referred to as ICT) system.

In order to encompass the issue of blocking internet content related to terrorism, it is crucial to determine how polish law defines terrorist offences. Under the provisions of Polish Criminal Code, a crime of a terrorist character is a prohibited act subject to maximum penalty of at least 5 years of deprivation of liberty, which is committed with the purpose of seriously terrorising a large number of people, compelling a public authority of the Republic of Poland, another state or an international organisation to perform or to refrain from performing certain actions, causing a serious disruption of the political system or economy of the Republic of Poland, of another state or an international organisation, as well as a threat to commit such an act[1682].

Important regulations of blocking access to content related to crimes with terrorist character in the Information and Communications Technology system can be found in the Internal Security Agency and the Foreign Intelligence Agency laws.

In order to prevent, counteract and detect terrorist offence described in Polish Criminal Code and also to prosecute their perpetrators, the Head of the Internal Security Agency may file a motion to the court, concerning blocking by the service provider of electronic services the accessibility of specific data related to a terrorist event in the ICT system or specific ICT services used to cause a terrorist event[1683]. This motion requires prior written authorisation of the Public Prosecutor General. The motion should contain in particular: the description of the incident of a terrorist nature, including its legal classification (if possible); the purpose and time of the blockade of access; circumstances justifying the need to block accessibility; a detailed description of the type of IT data or ICT services to be blocked; data allowing an unambiguous identification of the entity or the object concerned by the intended blocking and indicating the method of its implementation. All the above with other evidence justifying the necessity of an access block presented to the court. Only the District Court in Warsaw is legitimised to examine this kind of motion.

In urgent cases, if it could cause a terrorist event, the Head of the Internal Security Agency, having obtained the written authorisation of the Public Prosecutor General, may order blocking of access pending the court's decision.

1682 Article 115 §20 of the Act of 6 June 1997- Criminal Code [ustawa z dnia 6 czerwca 1997 r. Kodeks karny], Journal of laws of 1997, number 88, item 553, as amended.

1683 Article 32c of the Act of 24 May 2002 on the Internal Security Agency and Foreign Intelligence Agency [ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu], Journal of laws of 2002, number 74, item 676, as amended

If the court does not give its approval within five days or rejects the request, access must be unblocked.

The service provider of the services by electronic means is obliged to immediately perform the actions specified in the court's decision or the order of the Head of the Internal Security Agency. The accessibility blockade is ordered for no more than 30 days. If the reasons for order have not ceased, the court may, upon a written request of the Head of the Internal Security Agency (again with prior written authorisation of the Public Prosecutor General), issue a decision on the one-off extension of the access blockade. This blockade can be ordered for a maximum period of 3 months.

Access blockades cease in case of expiry of the period for which they have been introduced; the court's refusal to authorise the Head of Internal Security's order of the access blockade or the court's refusal to grant an extension of the blockade of access. The Head of the Internal Security Agency and the Public Prosecutor General may appeal court decisions. In such a case, the provisions of the Code of Criminal Procedure apply.

Those provisions constitute the procedure of content blocking, which may apply to the availability of both - specific ICT data and specific ICT services used to cause a terrorist event. The goal of combating terrorist crime is noble but polish legislators used very inclusive concepts of 'ICT data and services' and one can imagine using those provisions to block not only specific content but also entire websites.

2.2. Polish Press Law Act in the context of internet regulations

Another polish act that regulates the question of internet content is the Press Law Act of 1984. It is easy to see that this act is outdated. Over the past 36 years, there has been great technological progress. Especially in such a dynamically changing matter as the Internet, we need many adjustments in order to adapt the law to this progress. Although the press law regulation seems archaic, both the doctrine and the jurisprudence are of opinion that some transmissions of information on the Internet might be qualified as a press, therefore the provisions of the Polish Press Law Act should apply. This legislative solution is made possible by a broad and flexible definition of the press that takes into account technical progress. Press is defined as periodical publications that do not form a closed, homogeneous whole, appearing at least once a year, with a permanent title or name, current number, and date. They include in particular: newspapers and magazines, agency services, or newsletters; as well as all existing and resulting from technical progress mass media, such as broadcasting and radio stations, disseminating periodical publications through printing, video,

audio or other dissemination techniques[1684]. The Supreme Court of the Republic of Poland upheld the view almost unanimously recognised in the legal literature and in the case under the number III KK 250/10 stated that 'Transmission via the Internet, if it meets the requirements set out in Article 7 section 2 points 1 of the Act of 26 January 1984 - Press Law, is a press[…]'. The legislator introduced Press Law Act chapter 8 entitled 'Proceedings in press matters'. Unfortunately, it is difficult to argue that these provisions are exhaustive, as they have fragmentary and incidental nature. One should rather take the position that the Press Law Act only slightly modifies the procedural provisions relevant to a given branch of law. This is the reason why Article 50 provides for that to the legal proceedings arising from the Press Law Act general principles apply[1685]. This leads to the adoption of particular solutions discussed below.

2.3. Polish Civil Code

Polish law protects so-called personal interests. Those interests are enumerated in Article 23 of the Polish Civil Code and include in particular: health, freedom, dignity, freedom of conscience, surname or pseudonym, image, the confidentiality of correspondence, the inviolability of the privacy of one's home, as well as scientific, artistic, inventive and reasoning activities. They are protected regardless of the means of the violation, therefore including the internet.

A person whose personal interests are jeopardised by another person's action may demand, among others, to abandon the action. In the case of actual violation, it is also possible to demand that the responsible person performs acts necessary to remove its consequences[1686]. An example of such remedy may be: 1) a request to remove a specific internet publication or 2) a request to make a statement of specific content and in a specific form by a person who committed a violation.

In the first place, a person whose personal interests were violated should request to remove the content in violation. In the event of refusal, the case should be taken to civil court. Afterward, the court can order the removal of harmful internet publication or making a corrective statement. In the sentencing part of the judgment, the court determines the manner in which the defendant has to apologise as well as its exact wording.

1684 Article 7 section 2 of the Act of 26 January 1984 - Press Law [ustawa z dnia 26 stycznia 1984 r. Prawo prasowe], Journal of laws of 1984, number 5, item 24, as amended.

1685 M. Olszyński, Prawo Prasowe. Komentarz Praktyczny, LexisNexis 2013

1686 Article 24 § 1 of Act of 23 April 1964 Civil Code [ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny], Journal of laws of 1964, number 16, item 93, as amended.

It happens frequently that it is difficult to determine who is the author of harmful content. In this regard provisions of the act addressed below are useful.

2.4. Act on Electronically Supplied Services

A regulation set out in the Act on Electronically Supplied Services creates a well-thought-out mechanism. In the case of the unlawful character of the data, the victim may request to remove harmful content directly from the service provider.

In general, an entity that supplies the services is not obliged to check the data which are received, stored or transmitted by him[1687], which is understandable. It would be difficult if not impossible for the owners of the website to read all the users' posts. According to article 14, section 1 liability for stored data is not borne by someone making the resources of an information and communication technology system available for storing data by the customer, and who is not aware of the unlawful character of the data or related activities. Nevertheless, after receiving the information about content violating the law, the so-called 'notice and takedown' procedure occurs and access to said data should be blocked. Information on violation should be reliable and contain complete information that will allow the website administrator to make a full appreciation of the facts. A good solution is to indicate by websites in the terms and conditions how to report a violation and what information should be provided.

By complying with the obligation to block access to harmful content, service providers are released from liability. This article introduces an exclusion of liability for stored data, which is based on the provisions of civil law, criminal law and administrative law.

If the service providers do not comply with the request, the remain liable for the violation of a victim's personal interests.

Furthermore, the provisions of Act of Electronically Supplied Services authorise a service provider to provide a victim with the IP address and other information about the user who posted harmful content rendering determining the perpetrator possible, as the victim can pass this information to the police.

The provisions of the abovementioned article concern the entities that provide services of access to the resources of the ICT system to store data, (so-called web hosting). Therefore, this regulation applies to an entity that offers a space in the storage of an ICT system (e.g. a server) for data - so-called hosting

[1687] Article 15 of the Act of 18 July 2002 on Electronically Supplied Services [Ustawa z dnia 18 lipca 2002 r.o świadczeniu usług drogą elektroniczną], Journal of laws of 2002, number 144, item 1204, as amended.

provider. In polish doctrine, the notion of hosting provider is understood broadly. It means that entities providing the hosting service are not only those who store entire web pages for the service provider but also those who allow users to add content to their web pages, e.g. movies, photos or comments. With such approach hosting provider is also, for example, the owner of a social networking site in relation to the content provided by users; forum organiser in relation to the content of posts appearing on it, or the owner of a portal that is a journal or magazine in relation to the comments appearing under the articles he added[1688]

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

Poland, for the time being, does not have any comprehensive legislation on blocking, filtering or taking down content available on the Internet. As already mentioned in the previous chapter, pursuant to Article 14 section 1 of the Act on Electronically Supplied Services access to certain data accessible online may be however prevented on a 'notice and takedown' basis by a service provider who renders his services by electronic means and who has received an official notification or reliable information about the unlawful nature of such data or activities related hereto. The aforementioned provision does not list precisely what kind of data can be made inaccessible indicating only that the data itself or activities related hereto should be of 'unlawful' nature. This ensures broad application of this provision to any data that can be considered as contrary to any provision of the law. Therefore, the grounds for blocking, filtering or taking down content available on the Internet can be found in numerous legal acts of both civil and criminal law, including:

1. Article 119 of the Polish Criminal Code which prohibits the use of violence against, or of unlawful threats directed towards, a group of people or a specific individual on the grounds of nationality, ethnicity, race, political opinion, religion, or belief;

2. Article 256 section 1 of the Polish Criminal Code which prohibits public promotion of a fascist or other totalitarian system of state, or incitation of hatred based on national, ethnic, race or religious differences;

[1688] W. Chomiczewski. Article 14. W: Komentarz do ustawy o świadczeniu usług drogą elektroniczną, [w:] Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw. LexisNexis, 2011.

3. Article 257 of the Polish Criminal Code which prohibits public insult of either a group of people or an individual on the grounds of their nationality, ethnicity, race, religion, or belief, and the violation of personal inviolability of another individual for these reasons;

4. Article 255a of the Polish Criminal Code which prohibits distribution or public presentation of content that could facilitate the commission of a terrorist offence with the intention that such an offence be committed;

5. Article 23 of the Polish Civil Code which provides protection of personal interests of a human being, in particular health, freedom, dignity, freedom of conscience, name or pseudonym, image, privacy of correspondence, inviolability of home, and scientific, artistic, inventive or improvement achievements;

6. Article 32c of the Act on the Internal Security Agency and Foreign Intelligence Agency which provides a possibility to block the availability of online data or online services related to a terrorist event or used to cause a terrorist event in order to prevent, counteract and detect terrorist offences and to prosecute their perpetrators;

7. Article 115 section 1 of Law on Copyright and Related Rights which prohibits assigning to oneself authorship or misleading another person as to the authorship of the whole or part of another person's work or performance;

8. Article 116 section 1 of Law on Copyright and Related Rights which prohibits distributing the original or a derived version of another person's work or a performance, or publically distorting such work, performance, phonogram, first fixation of a film or broadcast, without authorisation or against its terms and conditions;

9. Article 117 section 1 of Law on Copyright and Related Rights which prohibits fixing or reproducing the original or a derived version of another person's work, a performance, a phonogram, a first fixation of a film or a broadcast for the purpose of their distribution, without authorisation or against its terms and conditions.

As follows from the above, different content can be considered illegal under civil or criminal law, however at the same time, the same content may meet the prerequisites of unlawfulness of both civil and criminal provisions.

Safeguards ensuring a balance between censoring and freedom of expression are, above all, provided in the Constitution of the Republic of Poland. Freedom to express opinions, to acquire and to disseminate information is guaranteed by its Article 54 section 1. Section 2 of this Article prohibits preventive censorship of

the means of social communication and the licensing of the press. Protection of different human freedoms, including the freedom of expression is also the subject of Article 31 of the Constitution of the Republic of Poland. Its section 2 states that everyone is obliged to respect the freedoms and rights of others whereas its section 3 strictly regulates the circumstances in which such human freedoms can be restricted. It reads that any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. It also states that such limitations shall not violate the essence of freedoms and rights.

Regarding the safeguards, the Act on Electronically Supplied Services, mentioned already at the beginning of this chapter, raises some doubts. In general, an online service provider is not obliged to check the data that he receives, stores or transmits. However, once he receives a reliable notification that certain data is illegal, he is obliged to block the data under the 'notice and takedown' procedure. The law, however, does not precise what is *reliable* notification. In accordance with the general practice, the reliable notification should contain at least:

- complete and true details of the person or entity making the notification (including contact details);

- complete and true information enabling the online service provider to identify within his resources data that is unlawful or related to unlawful activity;

- true information on the reason why specific data or activity related hereto is considered to be unlawful.

The Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online underlines that hosting service providers have a particularly important role in combating illegal content on the Internet, as they store information provided by users of these services and at their request and make this information available to other users, often on a large scale. The Commission states that mechanisms for submitting notices to hosting service providers regarding content deemed illegal are an important means of combating illegal content on the Internet. However, it should be noted that it is to the sole discretion of such an online service provider to determine whether the notification he received is reliable. Also, once he is notified about the unlawful data and decides not to take it down, he becomes liable for such illicit activity and for the violation of a victim's rights. Therefore, to avoid risk of the consequences resulting from leaving the data deemed unlawful in a

received notification, in case of doubts, the online service provider is more likely to delete such data which can result in excessive censorship and infringement of rights and freedoms, especially freedom of expression.

In a case where content has been blocked or taken down from the internet, a person or an entity suffering from harm as a result of such action can bring a lawsuit with a civil court. Taking into consideration the complexity and protraction of court proceedings, it may be questionable whether the review constitutes effective protection of freedom of expression online. Also, it should be noted that an online service provider who banned certain content on a basis of a notification which he considered reliable shall not be liable for damage caused as a result of preventing access to this data.

Moreover, the above mentioned provisions of the Act on Electronically Supplied Services that allow arbitrary assessment of the online service provider whether the hosted data is or is not unlawful may be contrary to the requirement of a legal basis for any blocking measure set out by the ECtHR Chamber judgment in the case of *Ahmet Yildirim v. Turkey*, (18 December 2012[1689]). In this judgement the Court states that a prior restraint is only compatible with the European Convention on Human Rights if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses. There is in fact a guarantee of a judicial review (though only subsequent review) under the Polish law, however since the measure in question seems to be arbitrary, the judicial review of the blocking of access may not be sufficient to prevent abuses.

On the other hand, another measure stipulated by Polish law that enables blocking of online data – a motion to the court of the Head of the Internal Security Agency requesting blocking the availability of specific online data related to a terrorist event or used to cause a terrorist event[1690], as described in the previous chapter, seems to be compliant with the requirements of the European Court of Human Rights. It should be noted in particular that it provides a strict legal framework regulating the scope of a ban and the guarantee of a judicial review.

The responsibility of the online services provider for the content that he makes available has been the subject of Polish jurisprudence, especially in relation to online hate speech. In the judgment of 08 July 2011, the Supreme Court of

[1689] Application no. 3111/10

[1690] Article 32c of the Act of 24 May 2002 on the Internal Security Agency and Foreign Intelligence Agency [ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu]

Poland[1691] stated that an online service provider who gives a possibility to access the Internet for free and to post on his discussion portal, is responsible for the violation of someone else's personal interests on such portal, if he knew that a specific entry violates such interest and yet did not immediately prevent access to the entry (i.e. did not delete it immediately). The facts of the case were that groundless accusations have been made against the plaintiff regarding acts that he did not commit through a server belonging to a city hall. The judgement provided detailed interpretation of Article 14 section 1 of the Act on Electronically Supplied Services.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In Poland, the private sector plays a leading role in managing the Internet and content that is published in virtual space. In this respect, Poland fits in with the pan-European tendency according to which the responsibility for the development and innovation of the Internet rests largely with private entities[1692]. The consequence of this approach is the adoption by Poland of a number of regulations that allow public service providers to achieve their public goals. These regulations allow, among others, blocking and deleting Internet content in certain situations, often giving these entities the opportunity to limit the rights of free expression for Internet users. Despite this, the self-regulation of the internet market in Poland is not a process with special emphasis.

4.1. Self-regulation of the internet market in Poland

The IAB Poland Internet Industry Employers Association (hereinafter also referred to as: IAB Poland) is the most dynamically operating institution in the framework of building the self-regulation system for the Internet market in Poland. It is an organisation of entities from the Internet industry that represents their broadly understood interests. IAB Poland has over 230 members, among which are the largest Polish Internet portals and advertising agencies. IAB Poland is the fourth largest association of Internet industry employers in the world. Its main goal and mission are to support the activities of internet market participants and to popularise it[1693].

[1691] Judgment of the Polish Supreme Court - Civil Chamber of 8 July 2011, reference number: IV CSK 665/10

[1692] Communication from the Commission to the European Parliament and the Council - Internet governance: the next steps / * COM / 2009/0277 final */

[1693] <https://iab.org.pl/> [last access: 12/02/2020]

Due to the size and number of members that IAB Poland brings together, it is the undisputed pioneer in the field of Internet self-regulation in Poland. In the official position presented on the IAB Poland website, its president - Piotr Kowalczyk emphasises that 'Self-regulation [...] is the best solution giving much more opportunities than adopting legal acts that are not able to keep up with the development of technology and services offered on the Internet.'[1694]

IAB Poland introduces codes of good practices, standards and templates of specific documents, which are aimed at unifying market practices. Examples of acts building a self-regulation system within the Internet industry in Poland are:

- Code of Good Practice on detailed rules for the protection of minors in on-demand audiovisual media services[1695],

- Good practices of Internet projects[1696],

- Good SEO \ SEM practices[1697],

- Standard and Recommendations for Display Advertising[1698].

The standards resulting from the documents presented above are not imposed by a statute or other generally applicable regulations, but they are established by IAB. They contain sets of rules of conduct (in particular ethical and professional standards) as well as sets of requirements for entrepreneurs who have undertaken to comply with them. These acts have varying levels of detail. For example, the Standard and Recommendations for Display Advertising contain more detailed guidelines than the documents about good practice. Some of the acts, as for instance the Code of Good Practice on the detailed rules for the protection of minors in on-demand audiovisual media services, have been prepared in cooperation with the National Broadcasting Council[1699] and the Ministry of Digitization[1700].

Self-regulatory documents containing appropriately specified and enforceable standards, provide for the possibility of introducing an appropriate mechanism

---

1694 <https://iab.org.pl/standardy-i-dobre-praktyki/dobre-praktyki-iab-polska-w-zakresie-reklamy-behawioralnej/> [last access: 12/02/2020]

1695 <https://www.iab.org.pl/wp-content/uploads/2014/07/iab_kdp_vod_maloletni_2014.pdf> [last access: 19/02/2020]

1696 <https://www.iab.org.pl/wp-content/uploads/2014/01/Zaleceniaprojektyinternetowe.pdf> [last access: 19/02/2020]

1697 <https://www.iab.org.pl/wp-content/uploads/2014/01/SEO_Guidelines.pdf> [last access: 19/02/2020]

1698 <https://www.iab.org.pl/wp-content/uploads/2016/08/Standardy_IABPolska_2016.pdf> [last access: 19/02/2020]

1699 Polish state body guarding the freedom of speech and the right to information in the media.

1700 Polish government administration office created on 8 December 2015 from the transformation of the Ministry of Administration and Digitization.

in case of violation of the norms contained therein. This means that in the event of a violation of the Code of Good Practice on detailed rules for the protection of minors in on-demand audiovisual media services, IAB may directly request the entrepreneur to remove the violation. This introduces a mechanism that could potentially lead to the removal of specific content.

Nevertheless, self-regulation of the internet market in Poland is still a new and constantly developing issue[1701]. For now, the best manifestation of self-regulatory techniques used is the shift to entities providing electronic services the obligation to independently regulate internal procedures regarding the response to the publication of illegal content within the virtual space that they manage. The lack of such reaction and appropriate procedures may lead to the liability of a private entity for other people's content published on its server.

4.2. Responsibility of private entities for content published on their servers

The legal act regulating legal issues related to the provision of electronic services, including the obligations of the service provider related to the provision of such services, is the Act of 18 July 2002 on the provision of electronic services (hereinafter also referred to as: the Act[1702]). The current content of the Act is due to the amendment that took place in 2019[1703], which was caused by the need to adapt Polish legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation (hereinafter also: Regulation or GDPR)[1704]. Due to the specificity of the internet industry, it should be recognised that the recipients of the regulations are mainly private entities providing services in the field of the Internet industry.

This Act does not introduce rules on the liability of an Internet Service Provider for someone else's statements, as these can be inferred directly from the general provisions of civil law and case law of the European Court of Human Rights[1705],

---

1701 A. Ogrodowczyk, L. Żebrowska, E. Murawska-Najmiec, K. Twardowska, Samoregulacja i współregulacja jako metoda rozwiązywania napięć w relacjach rynek-regulator, Warszawa 2018 r., page 20-28

1702 Number in the Polish Official Gazette: Dz. U. 2002 Nr 144 poz. 1204

1703 Act of 21 February 2019 amending certain acts in connection with ensuring the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation (hereinafter also: Regulation or GDPR)

1704 Official Journal of the European Union: L 119/1

1705 Judgment of the European Court of Human Rights of 16 June 2015 in the case of *Delfi AS v. Estonia* (No. 64569/09, Legalis). In this ruling, the European Court of Human Rights ruled that it is permissible

but provides for exclusions of such liability. However, whether a particular entity is subject to exemptions will often depend on the procedures adopted internally by it.

Exclusions are regulated in Article 14 of the Act. The premise for exemption from the liability of the internet service provider for the data (content) that is made available on its servers is that it prevents access to that data, which in practice amounts to blocking or deleting some content.

The above mentioned Article 14 largely refers to private entities that provide hosting services, i.e. they provide server memory that is connected to the network to store data from recipients[1706]. Nevertheless, you can also refer to websites that allow their users to comment on certain content. Therefore, the said regulation concerns the liability that may be incurred by the entity being the service provider for the content (data) which is placed in the virtual space it offers by third parties who are recipients.

The Polish legislator, in Article 14 of the Act, established premises excluding the liability of entities providing electronic services. Paragraph 1 of the said Article stipulates that entities providing ICT system resources for the purpose of storing data by the recipient shall not be liable for their unlawful nature, unless they are aware of their unlawful nature. As a consequence of the above, private entities may be liable for unlawful data that is stored on their servers only if they know of their unlawful nature[1707]. The said provision also imposes on the private entity the obligation to immediately prevent access to unlawful data if it receives official notification or receives reliable information about the unlawful nature of the data or related activities.

The regulation thus constructed entitles the private entity to use repression in the form of removing or blocking certain content in situations where there is even a suspicion that certain content is unlawful.

The Act does not regulate the manner in which the entities referred to above should accept reports of infringements. There are also no procedures established to verify the credibility of accepted applications. In order to regulate these issues,

to assign responsibility for offensive entries posted in comments on the Internet to a news portal. Thus, the Court assumed that in the national legal order there may be tools to limit freedom of expression in a situation where content posted on the Internet is abusive and the administrator of the page on which it was placed did not prevent it from being made public.

[1706] page Podrecki, Prawo Internetu, page 211

[1707] K. Chałubińska-Jentkiewicz, Article 14 [in:] Świadczenie usług drogą elektroniczną. Komentarz, 2019, point 3

the service provider should independently create and introduce internal regulations.

However, a separate issue is the liability of the entity providing services electronically to the person whose content has been removed or blocked, i.e. often the one whose rights to free expression on the Internet have been violated.

4.3. The unlawful nature of the data

The Act of 18 July 2002 on the provision of electronic services does not define which data should be treated as unlawful. However, it seems that the concept of unlawfulness in relation to internet data should be understood in a broad way. The doctrine[1708] indicates that the data is unlawful in a situation where it is contrary to the law or principles of social coexistence. Therefore, it should be recognised that the data may acquire an unlawful nature both in a situation where their content is inconsistent with the current legal order, as well as when it was obtained or disseminated contrary to applicable law.

4.4. Ways of obtaining redress by people whose data has been deleted or blocked

In accordance with the general principles of civil law, the removal or blocking of content that has been entrusted by a third party to a private entity under a service contract may be considered as a breach of the provisions of such a contract. It should also be noted that the person who has placed on a specific website data that has been blocked or deleted, will suffer damage associated with the loss of access to them in the event of their blocking, or their total loss in the event of their removal. This state of affairs may result in liability for damages within the meaning of Article 471 of the Act of 23 April 1964 - Civil Code (hereinafter also as: the Civil Code[1709]), according to which the debtor is obliged to compensate for damage resulting from non-performance or improper performance of the obligation. In the present case, it should be considered that the hosting provider should be liable for the damage that the service provider would suffer in the event of improper performance of his obligation. It is also necessary to consider tortious liability, which is provided for in Article 415 of the Civil Code. Pursuant to this provision, anyone who caused damage to another person is obliged to repair it. This provision constitutes the general basis for liability for damages and may apply in every case in which the damage was caused by the culpable behavior of a third party[1710]. As it was mentioned earlier,

[1708] Ibid.

[1709] Number in the Polish Official Gazette: Dz.U. 1964 nr 16 poz. 93

[1710] B. Lackoroński, M. Raczkowski, Article 415 [in:] red. K.Osajda, Kodeks cywilny. Komentarz, 2020, admission

deprivation of access to data or their complete deletion may be treated as causing damage to the person who entrusted it to a private entity.

Claim for compensation for contractual liability under Article 471 of the Civil Code and for tort liability arising from Article 415 of the Civil Code, may appear cumulatively[1711]. A person who has suffered damage related to the loss of access to or deletion of data may choose a liability regime which he will use. This possibility results indirectly from Article 443 of the Civil Code, which says that the fact that the act or omission from which the damage resulted was non-performance or improper performance of a pre-existing obligation does not exclude the claim for compensation for tort, unless the content of the pre-existing obligation provides otherwise.

There are no legal solutions in Poland that would provide for a special procedure to allow republication of content that has been blocked or removed.

The possibility of claiming compensation from the entity providing the resources of the ICT system for the purpose of data storage, however, is limited. This entity will not always be liable for damage resulting from its activities.

4.5. Exclusion of the liability of a private entity towards the person whose data has been deleted or blocked

The Polish legislator has introduced provisions which exclude the liability of private entities for blocking or deleting their content in relation to the persons who have made this content available to its server in strictly defined situations. The aforementioned Article 14 in paragraphs 2 and 3 introduce such exemptions, while indicating specific circumstances in which they can be applied.

In accordance with Article 14 paragraph 2, the service provider who has received an official notification of the unlawful nature of the stored data provided by the recipient and has prevented access to such data, shall not be liable to that recipient for damage resulting from preventing access to such data. As it results from this provision, the deletion or blocking of data by a private entity will not cause its liability in the event that it will be notified of the unlawfulness of this data by the relevant state authorities. In such a situation, Polish law does not impose on this entity the obligation to inform the recipient about the impossibility of access to data that it uploaded to the system. In such circumstances, the customer may find out about the blocking or deletion of data only at the next attempt to use the service.

[1711] W. Czachórski [in:] System Prawa Cywilnego, t. III, part 1, page 703–704

However, according to Article 14 paragraph 3: 'The service provider who has obtained reliable information about the unlawful nature of the stored data provided by the recipient and has prevented access to such data, is not liable to that recipient for damage arising as a result of preventing access to such data, if he immediately notified the recipient of his intention to prevent access to them'. This means that the exclusion of the liability of a private entity may also occur if it obtains reliable information about the unlawful nature of the stored data. The doctrine[1712] comments that the regulation does not define what a reliable message is and what can be considered as such. In addition, it has not been clarified from whom such information may come[1713] or what form it should take[1714].

It is worth noting that in this case only the liability of the private entity will depend on whether it immediately notified the recipient of his intention to prevent access to the data (content) to which the reliable message concerned. As it has already been stated before, the subject's liability depends to a large extent on the internal procedures it uses.

It should be mentioned, however, that the Polish legislator does not introduce any remedies that could be used by a person whose data has been blocked or deleted. However, such measures may be provided for in the policy of the provision of electronic services.

The requirement to define the policy of the provision of electronic services and to make them available to the recipient free of charge before concluding a contract for the provision of such services, results from Article 8 of the Act. Pursuant to this provision, the service provider is obliged to provide services electronically in accordance with the policy. It is in the policy that, although not necessarily, specific procedures may be introduced enabling the recipient to introduce the possibility of its opposition in the event of blocking or deleting data provided by it. However, this remains in the sphere of internal regulations of electronic service providers.

[1712] K. Chałubińska-Jentkiewicz, Article 14… op. cit., point 4

[1713] The judgment of the District Court in Siedlce of 28 November 2013, reference number act: I C 1113/12, not public

[1714] K. Chałubińska-Jentkiewicz, Article 14… op. cit., point 4

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

Poland applies the right to be forgotten, which results directly from community law of the European Union. However, the provisions governing the proceedings in cases of personal data breach, including the right to be forgotten result from national regulations. Poland has also established a special supervisory body to enforce such rights.

5.1. On what basis is the right to be forgotten respected in Poland?

The legal act regulating in Poland issues related to the protection of personal data is the Act of 10 May 2018 on the protection of personal data (hereinafter also: the Act)[1715], which replaced the previously applicable Act of 29 August 1997 on the protection of personal data[1716]. The new act entered into force on 25 May 2018. Its establishment was connected with the adoption by the EU legislator of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation (hereinafter also: Regulation or GDPR)[1717].

Since the entry into force of the Regulation, every Member State of the European Union, including Poland, has been obliged to ensure its effective application in its legal order. The adoption of the new law was therefore the result of the need to adapt the Polish legal order to the standards arising from the Regulation. However, the Act regulates only those issues that have been submitted for regulation by the GDPR in national law and those for which the possibility of modification has been provided for[1718]. This condition results from the fact that the GDPR, which is an EU regulation, can be applied directly in the order of the Member States, and thus also in the Polish legal order. The direct possibility of using the GDPR in the Polish legal system meant that it was not necessary to include all the norms contained therein.

Examples of regulations that were not included in the new law is the right to be forgotten. This right results from Article 17 GDPR. This article, although it has no equivalent in the Polish law, is directly applicable.

[1715] Number in the Polish Official Gazette: Dz.U. 2018 poz. 1000

[1716] Number in the Polish Official Gazette: Dz.U. 1997 nr 133 poz. 883

[1717] Official Journal of the European Union: L 119/1

[1718] I. Szczepańska-Kulik, Opinia do projektu ustawy o ochronie danych osobowych (druk sejmowy nr 2410), Biuro Analiz Sejmowych Kancelarii Sejmu, page 1

The possibility of direct application of the GDPR results from Article 288 of the Treaty on the Functioning of the European Union, which says that (EU) regulations are of general scope, binding in their entirety and are directly applicable in all member countries. As a member of the European Union[1719], Poland is therefore obliged to comply with these provisions. Poland's obligation to comply with international law binding on it results from Article 9 of the Polish Constitution.

5.2 What is the right to be forgotten?

Due to the fact that Poland has not developed its own regulations regarding the right to be forgotten, this concept takes the meaning that has been given to it in Article 17 GDPR. Despite this, it should be noted that the national legal doctrine also influences the way of understanding the right to be forgotten in Poland. Comments of representatives of Polish legal thought give tips on how to interpret EU regulations, thus somewhat adapting them to Polish realities.

According to Article 17 GDPR, the Right to be Forgotten is understood as the right of the data subject to request the administrator to delete his/her personal data immediately[1720]. The administrator, if such a request is made, is obliged to delete, without undue delay, the personal data of the said person if one of the following circumstances occurs:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

- the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;

- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;

- the personal data have been unlawfully processed;

- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

- the personal data have been collected in relation to the offer of information society services.

The Right to be Forgotten is also connected with the obligation of the data controller who made it public to take appropriate actions to inform other

[1719] Poland has been a member of the European Union since 1 May 2004. The legal basis for Poland's accession to the European Union is the Accession Treaty signed on 16 April 2003 in Athens.

[1720] A. Nerka, Article 17 [in:] red. M. Sakowska-Baryła, Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Legalis, point 1

controllers processing this data that the data subject requests that these controllers remove all links to this data, copies this personal data or their replications[1721].

However, the Right to be Forgotten may be limited. Such restrictions include:

- exercising the right of freedom of expression and information;

- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- reasons of public interest in the area of public health;

- the need to process data for archival purposes in the public interest, scientific or historical research or for statistical purposes;

- the need to process data to determine, pursue and defend claims[1722].

If the right to be forgotten collides with one of the restrictions mentioned above, the data controller does not have to delete the data of the person to whom they belong, despite the fact that he/she has requested it.

As it results from the above, a person who wants to delete their personal data, e.g. from the Internet, has the right to request from the entity administering such data to delete it. The data controller is obliged to respond to such requests as soon as possible - within a maximum of one month. If it is impossible to answer within this period, the administrator is obliged to inform the person who wanted to exercise the right to be forgotten about the reasons for the extension of the deadline. If the administrator does not respond to the request or refuses to delete the data, the person who made the request has the right to lodge an appropriate complaint to the Polish supervisory authority whose competence is to enforce personal data protection rights.

As it follows from the above, the way of understanding the Right to be Forgotten in Poland results directly from EU regulations, and not from national law.

[1721] page Barta, M. Kawecki, page Litwiński, Article 17 [in:] red. page Litwiński, Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Legalis, point 13

[1722] A. Nerka, Article 17 [in:] red. M. Sakowska-Baryła, Ogólne rozporządzenie… op. cit., point 6

5.3. What authority is responsible for enforcing the right to be forgotten in Poland?

The supervisory authority competent in matters of personal data protection in Poland is the President of the Office for Personal Data Protection (hereinafter also: the President of the Office), who heads the Office for Personal Data Protection. It is a body created pursuant to the Act of 10 May 2018 on the protection of personal data. The said authority replaced the previously functioning Inspector General for Personal Data Protection, who headed the Office of the Inspector General for Personal Data Protection. The first Polish President of the Office was Dr. Edyta Bielak-Jomaa - a Polish doctor of law. Jan Nowak has been holding this function since 16 May 2019.

The President of the Office is the body competent to deal with complaints about violations of personal data protection regulations. Therefore, it is also the competent authority to deal with complaints about violations of the provisions on the right to be forgotten.

5.4. What does the procedure look like in Poland if the right to be forgotten is violated?

The person who submitted the request to delete personal data pursuant to Article 17 GDPR to the relevant data controller who processes these data and has not received a response or has received an unfounded negative response, may submit a complaint directly to the President of the Office for Personal Data Protection. The person whose rights have been violated may choose the way in which he/she will make the complaint. The complaint may be submitted in electronic form, in paper form or for the minutes directly at the seat of the Office for Personal Data Protection.

The procedure initiated as a result of submitting a complaint to the President of the Office is an administrative procedure to which the provisions of the Polish Act of 14 June 1960 - Code of Administrative Procedure[1723] should be applied. The proceedings are single-instance. This means that if the President of the Office issues a decision unfavorable to the entity submitting the complaint, that entity may not appeal to a higher authority. It is worth noting that in the Polish legal order, the principle of two instances of administrative proceedings results directly from Article 78 of the Polish Constitution and Article 15 of the Code of Administrative Procedure. However, Article 78 of the Constitution allows for

[1723] Number in the Polish Official Gazette: Dz. U. 1960 Nr 30 poz. 168

exceptions to the above rule[1724]. The issue of single-instance proceedings before the President of the Office is, however, still a very controversial issue, especially in Polish legal doctrine[1725].

The proceedings regarding the breach of the law on the protection of personal data ends with an administrative decision issued by the President of the Office. As it results from the considerations presented above, the issued decision is final. This means that it cannot be appealed against in the administrative course of the instance or a request for reconsideration. Such a decision has the right to lodge a complaint with the Provincial Administrative Court within 30 days of its delivery. Such a complaint is lodged through the President of the Office. The entry for the complaint is PLN 200.00 (around EUR 46.75), however, the person who submits it has the right to apply for the right to assistance, which includes exemption from court costs and the appointment of a lawyer, legal adviser, tax adviser or patent attorney. For proceedings before administrative courts, the Act of 30 August 2002 Law on proceedings before administrative courts[1726] shall apply.

5.5. Administrative decisions of the President of the Office

The administrative decisions of the President of the Office are important in Poland in the process of interpreting the provisions of the Regulation and the Act. With the increasingly longer application of the provisions on the right to be forgotten, many decisions have been issued in this area as well. The vast majority of decisions concern the processing of personal data on the Internet or other electronic databases.

One of the most important decisions regarding the right to be forgotten concerned the obstruction by one of the companies of exercising the right to withdraw consent to the processing of personal data[1727]. The President of the Office imposed a fine of PLN 201,000.00 (approximately EUR 46,984.59) on a company that has not implemented adequate measures to effectively withdraw consent to the processing of personal data and to exercise the right to be forgotten. The punished company used complicated mechanisms to withdraw consent given online, which misled those interested. The person who wanted to

[1724] In accordance with Article 78 of the Polish Constitution, each party has the right to appeal against judgments and decisions issued at first instance. Exceptions to this rule and the appeals procedure are specified by statute. It should be noted that procedural issues in proceedings regarding personal data protection are regulated by the Act of 10 May 2018, which introduces just such an exception

[1725] S. Szczepaniak, Article 7 [in:] red. M. Kawecki, Ustawa o ochronie danych osobowych. Komentarz, Legalis, point 4

[1726] Number in the Polish Official Gazette: Dz. U. 2002 Nr 153 poz. 1270

[1727] Decision of the President of the Office for Personal Data Protection of 16 October 2019, reference number: ZSPR.421.7.2019

withdraw the consent was to enter the link provided in the commercial information. After entering, however, he/she encountered many difficulties. In addition, the company processed the data of persons who were not its clients. The data of these persons were processed despite their explicit requests to stop such proceedings. In this respect, the President of the Office considered this to be a serious violation of the right to be forgotten. In addition to the financial penalty, the President of the Office ordered the company to adapt its regulations to the provisions of the GDPR.

Another important decision regarding the right to be forgotten is the decision on the complaint about irregularities in the processing of personal data by the Chief Police Commander in Warsaw, involving the processing of personal data at the National Center for Criminal Information[1728]. The applicant pointed to the lack of legal grounds for the processing of his personal data in connection with the blurring of the conviction in his case. In this case, the President of the Office clearly indicated that the information collected in police databases are processed in accordance with applicable regulations, and law enforcement authorities are not obliged to inform the person whose personal data may be collected and processed about the fact of processing this data as well as about the scope of processing or sharing this data[1729]. Complaints about the collection and processing of personal data in police bases are extremely common in Poland. This is demonstrated, for example, by the list of decisions issued by the President of the Office in similar matters, which is published on the official website of the Office for Personal Data Protection[1730]. These cases mainly concern the violation of the right to be forgotten.

Another decision, in which the issue of the right to be forgotten was an important issue, was the decision on the application for irregularities in the processing of personal data on the Internet Debt Exchange - public platform on which debt sale offers are announced[1731]. The applicant's personal data was placed on this type of platform in order to sell the claim related to her. The scope of data that was made public included: name, surname, address data in the form of an indication of the city and the name of the street where the applicant lived. The building and apartment numbers were not provided. However, the value of

[1728] The National Criminal Information Center is an organizational unit in the Polish Police Headquarters. The tasks performed by this body consist mainly of processing criminal information and maintaining databases on this subject.

[1729] Decision of the President of the Office for Personal Data Protection of 5 September 2019, reference number: ZSOŚS.440.40.2019.

[1730] <https://uodo.gov.pl/234> [last access: 30/01/2020]

[1731] Decision of the President of the Office for Personal Data Protection of 4 January 2019, reference number: ZSPR.440.631.2018.

the claim that was offered for sale was given, as well as information about its limitation period. In this case, the President of the Office refused to grant the applicant's request, arguing that in that case there were no grounds to establish any infringement. The President of the Office indicated that the applicant's personal data was obtained on the basis of specific provisions on the assignment of claims, and their processing was aimed at pursuing the creditor's specific legal interest. Therefore, there is not infringement in this case. This decision is important because the Internet Debt Exchanges in Poland are a relatively popular tool for trading receivables and the issue of sharing debtors' personal data on them has always been a controversial issue.

Therefore, as can be seen, on the basis of the above examples, the President of the Office as a supervisory body is very active in the process of interpreting the provisions on the protection of personal data, including provisions on the right to be forgotten. This activity should be assessed in the positive way.

6. How does your country regulate the liability of internet intermediaries?

Poland remains among those Member States in which the liability of internet intermediaries remains uncertain. These entities are collectively called Internet Service Providers, however the category is certainly not uniform. As specified in the Directive 200/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) there can be distinguished providers of the following services: mere conduit, caching, and hosting.

As stipulated in the Preamble, the Directive came to force with a view to a clear framework of rules relevant to the issue of liability of intermediaries for copyright. This solution - concerning limitation of liability of intermediaries in the online environment – was adopted for the first time in the American Digital Millennium Copyright Act of 1998, which excludes or limits the liability of intermediaries on the Internet only to the extent of copyright infringements.

While one might have assumed that this Directive should introduce and harmonise European legislations, in Article 15 one might read that Member States shall not impose a general obligation on providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

Poland implemented the above article in its system in even more laconic form, by stating that a provider of the services of mere conduit, caching or hosting is

not obliged to check the data he transmits, stores or makes available. Thus the act clearly determined that immunity from liability for those entities is not dependent on maintenance of due diligence on their part as it comes to monitoring of data being stored or transmitted. That does not mean that they do not bear any liability for the infringements on their platforms. According to the dominant view in the doctrine, the Internet Service Provider will be liable, however, not as a direct perpetrator, but based on Article 422 of the Polish Civil Code.

On the basis of the above provision, as much as three entities may be held liable (if they are not direct perpetrators): the one who persuaded the direct perpetrator of the damage to do it, the one who was helpful to the perpetrator of the damage, or the one who knowingly took advantage of the damage caused to the other. From a legal perspective all of them are - as a consequence - guilty, which is a premise of their responsibility. However, there must be a normal causal link between the culpable conduct of the above mentioned entities and the actor's conduct.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

The internet is a tool that plays an increasingly important role in every area of life. It concerns both citizens and the functioning of the state. Given the dynamic development of new technologies, it is hard to say what the shape of the Internet reality will look like in a few years. New solutions will be followed by new threats, now completely unknown to us. This makes it difficult to outline the possibility of the evolution of Internet regulations. It certainly has to be said that the legislator must keep up with this development. This task is undoubtedly difficult.

An idea worth considering is a separate law that comprehensively deals with the Internet. As it was mentioned before, Poland is a country that does not have one, general act holistically dealing with Internet regulations. Such a hypothetical act could include not only the solutions already discussed in separate acts, i.e. liability of Internet service providers or blocking of Internet content, but also regulations concerning e.g. Internet sales, consumer rights on the Internet, protection of personal data and protection of privacy on the Internet or advertising law. It could, therefore, be an act that takes a holistic approach to the

Internet. The idea of a separate Internet regulation seems to be particularly relevant from the perspective of the development of blockchain technology, cloud services, and the so-called e-government. The state and citizens are increasingly benefiting from the Internet, and it is beginning to be present in every area of life.

The creation of a single law would bring several benefits. First of all, from a purely legislative perspective, it is easier to make changes in one act only. The legislator is never able to predict everything. It would seem that especially in such a dynamically developing branch as the Internet, changes which are a reaction to new technological solutions should be introduced quickly and consistently. From a legislative point of view, changes can be introduced more efficiently if they can be done in just one law. Additionally, when regulations are included in one act, it is easier to notice possible contradictions between individual regulations and eliminate them. The main advantage of this solution is, therefore, greater coherence of the law.

Another advantage is the ease of moving around the regulations. This would be a convenience for citizens and people working in the law professionally. It is much easier to navigate through the provisions of just one law than to look for regulations scattered over several legal acts. Often citizens are not even aware of the fact that regulations that concern a specific case are contained in several legal acts. Collecting regulations in one act would certainly help people who do not come into contact with the law on a daily basis to find themselves in the regulations and often find out about their rights.

What is more, with the multitude of legal acts regulating the law of the Internet, it is easy to omit some regulations. Thanks to this solution, it would be easier to find out which regulations are lex generalis and which are lex specialis and which regulations should be applied in a given case. It would, therefore, be a procedural facilitation.

In addition, the legislator often uses referral rules. Here again, from a purely technical point of view, it would be easier to find the provisions to which the law refers if they are contained in a single piece of legislation.

As can be seen, the inclusion of regulations concerning the Internet in one act undoubtedly brings with it benefits, but like any solution, it also brings with it certain problems. It is obvious that such a holistic law would be a very extensive piece of legislation. It might seem that there are too many issues the law would have to address. This could hypothetically lead to a situation where regulations are too general. Moreover, it is also hard to imagine an act regulating such an extensive branch of law in both private and public relations.

In order to create it, it would require the cooperation of people specialising in specific areas of the Internet, both lawyers and IT specialists. Considering the completely different approach to both the law and the Internet, it is not difficult to imagine that work on a new law would take a very long time before a compromise is reached.

Additionally, it should be remembered that the law is a system of interconnected standards. It is impossible to isolate individual branches of law from each other. Despite the creation of a separate, holistic regulation concerning the law of the Internet, which would be internally coherent, all issues would have to be compatible with the entire legal system.

The prospect of a single law seems to be a long way off, but the idea is worth considering by the legislator. We have to point out again that the process of drafting such an act, requires highly qualified professionals from both Internet and Law markets who preferably are not involved in politics, so this new act would not be used as a political tool. It is easy to manipulate and create regulations favourable for specific individuals or groups in the process of making a new law that destined to regulate holistically one branch of law. That might potentially have further influence on others' freedom of expression.

Another conclusion that comes to mind after analysing Polish regulations on the Internet is the breadth of terms used in them. Some of them are defined at the statutory level (legal definitions), but there are many not defined anywhere, e.g. the previously mentioned 'hate speech'. Some of them are subject to doctrine considerations. Over the last few years, this has resulted in a rich body of work involving academic discussions and case law. This situation naturally causes numerous discrepancies in the interpretation of these concepts. This, in turn, results in the occurrence of uncertainty in legal transactions. Judgments often contradict each other. Researchers and practitioners postulate the need for change, and as mentioned earlier about the term 'hate speech', governing all grounds of discrimination might be enshrined in the Criminal Code. Moreover sex, gender identity, disability, and sexual orientation should be added to the list of protected grounds in the hate crime provisions.

Taking into account the above problem, the legislator could in the near future reflect on the statutory clarification of terms in the sphere of internet law.

Certainly, Internet regulations should be changed, adapted to the changing world. This is quite a challenge for the legislator, but constant modification is necessary to ensure the safety of citizens as well as the best possible conditions for enjoying the benefits of the Internet.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

8.1. The (non-)absolute character of freedom of expression

Freedom of opinion and expression are classified as fundamental rights of every human being. Not only are they indispensable for individual dignity and fulfillment but also constitute vital foundations for values such as democracy, rule of law and stability. This naturally means that states and their governments are obliged to respect, protect and promote them.

In Poland freedom of expression is guaranteed in Article 54 of the Constitution, which states that 'everyone is guaranteed the freedom to express their views and to obtain and disseminate information.' Importantly, paragraph 2 of the aforementioned article specifies that preventive censorship of the media and licensing of the press are prohibited. It can thus be stated that Article 54 constitutes an impartial and systematic means of protection against censorship in its various forms, and serves to promote standards for the protection of freedom of expression.

It is worth mentioning that the wording of the first paragraph of this article is, in fact, similar to the phrasing of Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which additionally highlights that freedom of expression includes the freedom to hold opinions and to receive and impart information 'without interference by public authority and regardless of frontiers.' That being said, it seems that the right to freedom of expression includes a dual concept: the right to hold opinions without any kind of interference and the freedom to seek and receive information.

While the scope of the right to freedom of expression is broad, one of the natural questions arising from this stance is that of the absolute character of this freedom. This issue has, in its subtlety, contributed to an interpretation in solid favor of freedom of speech. The aforementioned article of the polish constitution neither offers distinction nor elaborates on any possible legal circumstances that would trigger the adoption of a law by the legislative body limiting the freedom of expression *per se*.

An example of one of the possible answers to the question above can be found in the structure of Article 31 which enounces the legitimate aims that can justify the restriction of any constitutional freedom, i.e. 'national security or public order; the natural environment; public health or public morals; or the rights of

others.' It should be emphasised that any restriction or limitation imposed by the State on the right to freedom of expression must conform to the strict requirements: it must be provided by law, introduced only if necessary and under no circumstances should it violate the substance of specific freedom.

In this context, from a legal perspective, 'hate speech' might be covered by freedom of expression.

8.2. Prohibitions of 'hate speech' in Polish law

While 'hate speech' has no legal definition under Polish law, as a Member of European Union, Poland is obliged to respect EU Conventions that prohibit discrimination and – thus: hate speech directed towards an individual or a group (distinguished based on a protected characteristic) is regulated by certain provisions, scattered among different legislative acts. Nevertheless, the internet remains a new field of communication in which a limited number of separate regulations have been adopted at the national level. Therefore, as it will be elaborated below, national judges play a major role in establishing standards on the protection concerning expression in an online environment.

8.2.1. The hate speech definition dilemma

While the concept of freedom of speech has been largely discussed and scholars agree on its special value, the concept of hate speech remains highly debated.

The District Court in Warsaw in the reasoning of the judgment of 14 August 2013[1732] generally referred to hate speech issues, pointing out that 'the concept [of hate speech] is defined in doctrinal interpretation. It is understood that hate speech stands for written, oral or symbolic statements that makes the subject of attack an individual or a group of people distinguished by the criteria of race, ethnicity, nationality, religion, language, gender, age, disability, external characteristics, sexual orientation and gender identity, social status or political beliefs. Hate speech can intimidate, threaten, humiliate, insult, perpetuate stereotypes and lead to discrimination and even physical violence.' In the quoted passage of reasons, the Court also gave criteria to determine who can become a victim of hate speech on a legal basis. It should be noted that the Court only defined what type of speech (i.e. 'written, oral or symbolic statement') falls within the term, without elaborating on the hate speech definition issue itself.

On the other hand, in the reasoning of the judgment of 4 August 2009[1733], the District Court in Szczecin pointed out that 'hate speech aims to consolidate the

[1732] Judgment of the District Court in Warsaw of 14 August 2013, XX GC 757/12.
[1733] Judgment of the District Court in Szczecin of 4 August 2009, I C 764/08.

negative and untrue image of certain [in this case: homosexual] persons in the public opinion.'

Subsequently, the Polish Supreme Court referred to the issue of 'hate speech' on the Internet in its judgment of 30 September 2016[1734], stating that: 'freedom of expression exercised on the internet forums by anonymous authors often provokes unrestrained statements that turn into so-called 'hate speech', that violates the personal rights of third parties'.

In recent case law, it was, however, also highlighted that 'hate speech' is commonly understood as statements and images that are abusive, mocking and humiliating groups and/or individuals for reasons wholly or partly independent of them[1735].

While the content of the abovementioned judgments indicates that the courts did not necessarily have to analyse certain behaviors as 'hate speech', since referring to this concept was not relevant to establishing the violation of certain rights, it should be noted, however, that without clear definition of the term, identifying instances of it in practice might prove difficult, specifically when it comes to cases of the 'hate speech' on the Internet.

8.2.2. Prohibitions in light of the criminal law

The Polish Criminal Code contains several provisions indirectly restricting some forms of 'hate speech', including:

- Article 119 which prohibits the use of violence against, or of unlawful threats directed towards, a group of people or a specific individual due to one's nationality, ethnicity, race, political opinion, religion, or belief;

- Article 256 paragraph 1 which prohibits publicly promoting fascist or any other totalitarian regime or provoking to hatred on the grounds of nationality, ethnicity, race, religion or belief, and;

- Article 257 which prohibits public insult of either a group of people or an individual on the grounds of their nationality, ethnicity, race, religion, or belief, and the violation of personal inviolability of another individual for these reasons.

As one might notice, none of the above mentioned articles addresses 'hate speech' in the online environment. Additionally, it might be noticed that criminal provisions do not regulate the 'hate speech' phenomenon exhaustively. The list of protected features is exhaustive but limited to nationality, ethnicity, race, religion, or belief. Thus, other categories, such as sex, gender identity are not

[1734] Judgment of the Supreme Court of 30 September 2016, I CSK 598/15.
[1735] Judgement of the Supreme Court of 8 February 2019, IV KK38/18.

included in these provisions, resulting in discrepancies in prosecuting and sentencing of hate crimes in general.

The absence of the above grounds in the provisions on hate speech and hate crime results in offences targeting, e.g. LGBT people, being prosecuted as common crimes and in consequence, they and are not always prosecuted *ex offcio,* as it is in the case of racist crimes.

Moreover, as M. Woiński highlights 'the current provisions on racist threats, violence and incitement to hatred were largely copied from the Polish Criminal Code from 1969, where they were introduced following the experience of the World War II and remained unchanged for almost 50 years, despite the immense political changes in Poland[1736]'.

However, it should be also noted, as already stated, that in more recent case law, courts are more eager to extend the scope of the above articles, Article 256 in particular. According *inter alia* to the judgment of 8 February 2019, Article 256 should be interpreted broadly and its subject of protection are the rules of democracy. Proper functioning of the state requires protection against ideological threats and hate-based antagonisms, and thus 'hate speech' originating from intolerance may be sanctioned under this article[1737]. On the other hand, the ruling does not explicitly determine whether the term 'intolerance' includes any form of intolerance (meaning also those arising from gender affiliation and on other basis not enumerated in the article) or not.

8.3. Striking a balance

The fact that hate speech can interfere with human rights and other basic values, such as dignity or equality is undebatable. Nonetheless, there are no legislative initiatives underway to amend the existing provisions related to 'hate speech' under the Criminal Code, even though, in recent years, human rights non-governmental organisations and academics have continuously advocated in support of such.

When it comes to combating hate speech the elements of the necessary actions are fairly easy to indicate – they can be found in the reports published by the regional and international monitoring bodies, such as e.g. the Human Rights Committee.

First of all, the definition of hate speech governing all grounds of discrimination should be enshrined in the Criminal Code - and accordingly - sex, gender

[1736] Mateusz Woiński, Prawnokarne Aspekty Zwalczania Mowy Nienawiści [Criminal Law Aspects of Combating Hate Speech] (Warszawa: LexisNexis, 2014), 156–57.
[1737] Judgement of the Supreme Court of 8 February 2019, IV KK38/18.

identity, disability and sexual orientation should be added to the list of protected grounds in the hate crime provisions.

Secondly, criminal provisions should specifically define acts that could be subject to criminal proceedings in cases of 'hate speech' and consequently all types of such offences committed with a bias motive should be investigated *ex officio*.

Additionally, when it comes to the online environment and specifically hate crimes committed on the internet, the web administrators should be obliged to monitor the content of their websites and counteract hate speech that may later result in hate crimes.

Such efforts need to be located in a broader perspective – they need to be part of a wide-ranging commitment and investment in society – hence polish government should first and foremost conduct intensified awareness-raising campaigns about hate speech and hate crimes.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

9.1. Freedom of expression and the right to privacy

Freedom of opinion and expression are vital human rights in any well-functioning democracy. As it has already been stated above, they constitute vital foundations for values such as democracy, rule of law and stability. Free speech is thus a necessary precondition to the enjoyment of other rights. On the other hand, freedom of expression may clash with other fundamental rights enshrined in the national legal systems.

In Poland freedom of expression is guaranteed by the Constitution. While, Article 54 specifies that everyone is guaranteed the freedom to express their views and to obtain and disseminate information, another Article – namely Article 47 – ensures legal protection of private life for everyone by stating that 'everyone has the right to the legal protection of private and family life, honor and reputation, and to decide on their personal lives.'

The Right to Privacy is included in the chapter relating to fundamental rights and freedoms. It is also protected directly under provisions of Polish Civil Code (Article 23 and 24).

It should be noted that privacy as a value *per se* should be seen rather as constitutional freedom (and not as a right) since it is inherent and exists

regardless of the will of the legislator. Legal acts, by declaring the existence of the right to privacy, do not create it, but only guarantee it. The right to privacy should be thus interpreted as an obligation imposed on the State to take action to secure the private life sphere against interference by third parties. Additionally, in normative sense, it presupposes the right to form one's private sphere so that it is inaccessible to the others.

The delicate balance between a person's right to privacy and someone else's right to freedom of expression oftentimes might result in collision. The question emerges: which one of those rights prevails and how Polish judiciary balance the potentially competing interests of personal privacy and free expression?

In principle, the two rights have equal weight -which right prevails depends on the circumstances of a case. Determining the proper balancing of these two rights is, however, challenging, particularly when it comes to public information, on which journalists believe to have the right to publicise. One might argue that, in fact, in relation to public information, which is by definition 'publicly available' the right to freedom of expression should be given free reign.

Polish legal system guarantees the right to obtain information on the activities of the authorities performing public functions and the right to protection of personal data, arising from Article 51 of the Constitution. These rights are associated with obligations on the part of the authorities, which allows their implementation.

On the other hand, Article 14 of the Press Law Act stipulates that it is not allowed to publish information and data regarding a private sphere of an individual without the consent of the person concerned, unless it is directly related to their public activities.

However, the Internet cannot be fully subjected to rules dictated by press law and as a consequence it cannot be fully regulated by press law.

Therefore, an assessment of relation between information distributed via internet and public activity of a specific person (with regards to potential infringements of the Right to Privacy) should each time be submitted to the court's decision, as regards the objective and potential consequences of the distribution.

9.2. Striking a balance

When analysing the issue violation of privacy with regards to the freedom of expression, it would be more appropriate to perceive the Internet from a broader viewpoint than just press law. The Internet is a new field of communication, that

allows violations of the right to privacy to occur on a different level - outside of press *sensu stricte*, i.e. on personal blogs, social media profiles.

It should be also noted that in the digital societies, as well as in Polish legal system, privacy protection corresponds closely with the system protection of information and personal data. Threats to privacy nowadays primarily concerns the functioning of modern information systems, based on their operation on electronic data processing techniques. Data processing and storage increase the risk for personal data and privacy.

Therefore, first and foremost the State should oblige the web administrators to thoroughly and strictly monitor the content of their websites.

At the same time, coherent national regulation on the above matters regarding the right to privacy specifically in the online environment should be established.

10. How do you rank the access to freedom of expression online in your country?

On a scale of 1 to 5, I rank the access to freedom of expression online in Poland at 4.

First of all, Poland does not have specific acts on blocking and taking down of content on the internet. This leads to the situation when we have a number of rules scattered across different acts which definitely disturbs the transparency of regulations. Nevertheless, there are reasons why content on the internet may be blocked. One of them is blocking the accessibility of data related to a terrorist crime in the ICT system. Content can also be removed when it violates the personal interests of another person, like health, freedom, dignity, freedom of conscience,

surname or pseudonym, image, the confidentiality of correspondence, the inviolability of the privacy of one's home, as well as scientific, artistic, inventive and reasoning activities. It is worth recalling here a universal principle that says that one person's freedom ends where the other person's freedom begins. Also, according to regulation set out in the Act on Electronically Supplied Services, in the case of the unlawful character of the data, the service provider may delete content requested by the victim of the violation. What is interesting, in the judgment of 24 November 2017, the Supreme Court of Poland[1738] states that the administrator is responsible for their own actions that violate the personal rights

[1738] Judgment of the Polish Supreme Court - Civil Chamber of 24 November 2017, reference number: I CSK 73/17

of third parties, which involve the dissemination and maintenance of someone else's anonymous information violating those rights via the website. The provision of Article 14 paragraph 1 of the Act on Electronically Supplied Services excludes the administrator's responsibility when he does not know about the unlawful nature of the data stored and shared using the hosting services. The source of knowledge about unlawful comments need not come from the victim. The administrator's knowledge should also include the situation when the administrator, in view of his experience in hosting, assumes on the possibility for internet users to post comments that violate the personal rights of specific persons. [1739]

Second, it is also important to highlight aspects related to 'hate speech'. In Polish law there is no legal definition of this term. Additionally, criminal provisions do not regulate 'hate speech' phenomenon exhaustively. Such a situation creates problems with the penalisation of 'hate speech'. Even if judicial decisions play an important role in establishing standards on the protection concerning expression online, this does not change the fact that we still do not have any legal act that directly relates to hate speech. This can sometimes even lead to the abuse of freedom of expression online.

Moreover, attention should also be paid to constitutional regulations. Referring to Article 54 of the Constitution, you may notice that the limits of the right to freedom of expression go far enough. This right includes: the right to hold opinions without any kind of interference and the freedom to seek and receive information. Article 54 does not provide regulations restricting freedom of expression. Such regulations can be found in Article 31 of the Constitution, but it should be noted that restrictions on freedom may only take place for valid reasons and in compliance with strictly defined procedures.

To sum up, access to freedom of expression online in Poland is very wide, but does not have absolute character. Situations that justify restricting freedom of expression online can be found in Polish regulations. Nevertheless, I believe that each of these situations is fully justified, such as terrorism or violation of the rights of another person.

[1739] Judgment of the Polish Supreme Court - Civil Chamber of 30 September 2016, reference number: I CSK 598/15

11. How do you overall assess the legal situation in your country regarding internet censorship?

In all legal systems around Europe, there are laws or administrative practices that can be used to ban or censor certain contents both on- and offline.

As stated above in this report, the internet remains a new field of communication in which a limited number of separate regulations have been adopted both at the international as well as national level.

While Polish legal system, like almost all current European democracies, regulates matters regarding privacy protection of natural persons or freedom of expression, Poland also remains one of the EU Member States that do not have one specific legislation on blocking and taking down of content on the internet. This stance does not naturally imply absence of any provision regarding censorship. Polish legal system, however, lacks a general act that would harmonise the rules on internet censorship and the numerous rules are scattered across different acts.

One might think that those vague and broad provisions are only aimed to cause confusion and ultimately e.g. facilitate the removal of undesirable content or restrict the right to freedom of expression of certain individuals. However, it should be noted that the above situation is rather a result of generally little tradition on the matters such as freedom of speech or right to privacy in Poland, rather than deliberate actions of the legislator to limit fundamental freedoms.

Nonetheless, it should be also highlighted, that media self-regulation concerning e.g. 'hate speech' is largely ineffectual in Poland and at the same time, there are no legislative initiatives underway to amend e.g. the existing Polish provisions related to 'hate speech' in the online environment, even though, in the recent years, human rights non-governmental organisations and academics have continuously advocated in support of such.

To sum up, as highlighted in this report, the legal and policy framework relating to the internet is not sufficient to comprehensively respond to certain instances of infringements that occur in an online environment. Therefore, all relevant Polish legislation related to the above described legal matters should be revised for their compliance with international standards concerning digital environment.

Conclusion

When it comes to the balance between a person's freedom of expression and someone else's right to privacy the main problem is that these two rights have equal weight, so it depends on the circumstances of a case in which one of them prevails. Finding a proper balancing of these two rights is challenging, especially when it comes to public information. It should be also noted that in the digital societies, as well as in Polish legal system, privacy protection corresponds closely with the system of protection of information and personal data. Coherent national regulation on the above matters regarding the right to privacy specifically in the online environment should be established.

It is also important to highlight aspects related to hate speech. In Polish law there is no legal definition of this term and criminal provisions do not regulate 'hate speech' phenomenon exhaustively which can sometimes lead to the abuse of freedom of expression. Such a situation creates problems with it is penalisation, even though judicial decisions play an important role in establishing standards of the protection of personal rights.

As stated above in this report, the Internet provides a new field of communication in which a limited number of separate regulations have been adopted. The legal and policy framework relating to the Internet are not sufficient to comprehensively respond to certain instances of violation that occur in an online environment. Therefore, all relevant Polish legislation related to the matters described above should be revised for their compliance with international standards concerning digital environment. Poland still remains one of the EU countries that do not have one specific legislation on blocking and taking down of content on the Internet which leads to the situation where we have numerous regulations scattered across different acts and that disturbs the transparency of these regulations. Such act could include not only the solutions like liability of Internet service providers or blocking of Internet content, but also regulations concerning e.g. Internet sales, consumer rights on the Internet, protection of personal data and protection of privacy on the Internet or advertising law.

Table of legislation

Provision in Polish language	**Corresponding translation in English**
Konstytucja Rzeczpospolitej Polskiej, artykuł 54: 1. Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. 2. Cenzura prewencyjna środków społecznego przekazu oraz koncesjonowanie prasy są zakazane. Ustawa może wprowadzić obowiązek uprzedniego uzyskania koncesji na prowadzenie stacji radiowej lub telewizyjnej.	The Constitution of the Republic of Poland, Article 54: 1. The freedom to express opinions, to acquire and to disseminate information shall be guaranteed to everyone. 2. Preventive censorship of the means of social communication and the licensing of the press shall be prohibited. Statutes may require obtaining a permit for the operation of a radio or television station.
Konstytucja Rzeczpospolitej Polskiej, artykuł 31 ustęp 2 i 3: 2. Każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje. 3. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.	The Constitution of the Republic of Poland, Article 31 Section 2 i 3: 2. Everyone is obliged to respect the freedom and rights of others. No one may be forced to do what the law does not mandate him. 3. Any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights.
Konstytucja Rzeczpospolitej Polskiej, artykuł 61: 1. Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. 2. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z	The Constitution of the Republic of Poland, Article 61: 1. A citizen has the right to obtain information on the activities of the organs of public authority as well as persons exercising public functions. Such rights include obtaining the information on the activities of local government's bodies - economic or professional organs and other persons or organisational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury. 2. The right to obtain information ensures access to documents and entry to sittings of collective organs of public authority formed by universal elections, with the opportunity to make sound and visual recordings.

powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu. 3. Ograniczenie prawa, o którym mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa. 4. Tryb udzielania informacji, o których mowa w ust. 1 i 2, określają ustawy, a w odniesieniu do Sejmu i Senatu ich regulaminy.	3. Limitations upon the rights referred to in sections 1 and 2 above, may be imposed by the statute solely to protect freedoms and rights of other persons and economic subjects, public order, security or important economic interests of the State. 4. The procedure of providing the information referred to in sections 1 and 2 above are specified by the statute, and regarding the Sejm and the Senate by their regulations.
Konstytucja Rzeczpospolitej Polskiej, artykuł 2: Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej.	The Constitution of the Republic of Poland, Article 2: The Republic of Poland is a democratic state of law, implementing the principles of social justice.
Konstytucja Rzeczpospolitej Polskiej, artykuł 9: Rzeczpospolita Polska przestrzega wiążącego ją prawa międzynarodowego.	The Constitution of the Republic of Poland, Article 9: The Republic of Poland shall observe international law binding on it.
Konstytucja Rzeczpospolitej Polskiej, artykuł 78: Każda ze stron ma prawo do zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji. Wyjątki od tej zasady oraz tryb zaskarżania określa ustawa.	The Constitution of the Republic of Poland, Article 78: Each part has right the right to appeal against judgements and decisions issued at first instance. Exceptions to this rule and the appeals procedure are specified by statute.
Ustawa z dnia 6 września 2001r. o dostępie do informacji publicznej, artykuł 1: Każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w niniejszej ustawie.	Act of 6 September 2001 on access to public information, Article 1: Any information on public matters constitutes public information in the meaning of the statute and is subject to disclosure on the terms and in the manner specified in this statute.
Kodeks karny, artykuł 119: Kto stosuje przemoc lub groźbę bezprawną wobec grupy osób lub poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, politycznej, wyznaniowej lub z powodu jej bezwyznaniowości, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.	Polish Penal Code, Article 119: Whoever uses violence or an unlawful threat against a group of people or an individual because of his nationality, ethnicity, race, politics, religion or because of his denominationality, is subject to detention from 3 months to 5 years.

Kodeks karny, artykuł 256 §1: Kto publicznie propaguje faszystowski lub inny totalitarny ustrój państwa lub nawołuje do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.	Polish Penal Code, Article 256 par. 1: Whoever publicly propagates a fascist or other totalitarian state system or agitates to hate based on national, ethnic, racial, religious differences or because of lack of religious denomination, is subject to a fine, restriction of liberty or detention up to 2 years.
Kodeks karny, artykuł 257: Kto publicznie znieważa grupę ludności albo poszczególną osobę z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości lub z takich powodów narusza nietykalność cielesną innej osoby, podlega karze pozbawienia wolności do lat 3.	Polish Penal Code, Article 257: Whoever publicly insults a group of people or a particular person because of their national, ethnic, racial, religious affiliation or because of their lack of religious denomination or for such reasons violates the physical integrity of another person, is subject detention up to 3 years.
Kodeks karny, artykuł 255a: §1. Kto rozpowszechnia lub publicznie prezentuje treści mogące ułatwić popełnienie przestępstwa o charakterze terrorystycznym w zamiarze, aby przestępstwo takie zostało popełnione, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. §2. Tej samej karze podlega, kto w celu popełnienia przestępstwa o charakterze terrorystycznym uczestniczy w szkoleniu mogącym umożliwić popełnienie takiego przestępstwa.	Polish Penal Code, Article 255a: Par. 1. Whoever disseminates or publicly presents content that may facilitate the commission of a terrorist offense with the intention that such offense would be committed, is subject to detention from 3 months to 5 years. Par. 2. The same punishment shall be imposed on anyone who, in order to commit a terrorist offense, participates in training that enables the commission of such an offense.
Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną, artykuł 14: 1. Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych. 2. Usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do	Act of 18 July 2002 on Rendering Electronic Services, Article 14: 1. The person, who provides access to the ICT system resources in order to store data by the recipient, is not aware of the unlawful nature of the data or related activities, and in the event of receiving official notification or obtaining reliable information about the unlawful nature of the data or related activities will prevent access to this data, shall not be liable for stored data. 2. The service provider who has received an official notification of the unlawful nature of the stored data provided by the recipient and has prevented access to such data, shall not be liable to that recipient for damage

tych danych, nie ponosi odpowiedzialności względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych. 3. Usługodawca, który uzyskał wiarygodną wiadomość o bezprawnym charakterze przechowywanych danych dostarczonych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada względem tego usługobiorcy za szkodę powstałą w wyniku uniemożliwienia dostępu do tych danych, jeżeli niezwłocznie zawiadomił usługobiorcę o zamiarze uniemożliwienia do nich dostępu. 4. Przepisów ust.1–3 nie stosuje się, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów o ochronie konkurencji i konsumentów.	resulting from preventing access to such data. 3. The service provider who has obtained reliable information about the unlawful nature of the stored data provided by the recipient and has prevented access to such data, is not liable to that recipient for damage arising as a result of preventing access to such data, if he immediately notified the recipient of his intention to prevent access to them. 4. The provisions of paragraphs 1-3 shall not apply if the service provider has taken control of the recipient within the meaning of the provisions on competition and consumer protection.
Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną, artykuł 15: Podmiot, który świadczy usługi określone w Article 12–14, nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych, o których mowa w Article 12–14.	Act of 18 July 2002 on Rendering Electronic Services, Article 15: The entity that provides the services referred to in Articles 12–14 is not obliged to check the data, referred to in Articles 12–14, which is provided, stored or shared by it.
Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną, artykuł 8: 1. Usługodawca: 1) określa regulamin świadczenia usług drogą elektroniczną, zwany dalej „regulaminem"; 2) nieodpłatnie udostępnia usługobiorcy regulamin przed zawarciem umowy o świadczenie takich usług, a także – na jego żądanie – w taki sposób, który umożliwia pozyskanie, odtwarzanie i utrwalanie treści regulaminu za pomocą systemu teleinformatycznego, którym posługuje się usługobiorca. 2. Usługobiorca nie jest związany tymi postanowieniami regulaminu, które nie zostały mu udostępnione w sposób, o którym mowa w ust. 1 pkt 2. 3. Regulamin określa w szczególności: 1) rodzaje i zakres usług świadczonych drogą elektroniczną; 2) warunki świadczenia usług drogą elektroniczną, w tym:	Act of 18 July 2002 on Rendering Electronic Services, Article 8: 1. A service provider: 1) establishes regulations for providing services by electronic means referred hereinafter as "the regulations", 2) makes available the regulations to a service recipient free of charge before concluding the contract on providing such services, and also - on his/her request - in such a manner, which enables downloading, retrieval and saving contents of the regulations through the teleinformation system used by the recipient. 2. A service recipient shall not be bound by the provisions of the regulations, which have not been made available to him/her in the manner referred to in paragraph 1 point 2. 3. The regulations specifies in particular: 1) types and scope of services provided by electronic means,

a) wymagania techniczne niezbędne do współpracy z systemem teleinformatycznym, którym posługuje się usługodawca, b) zakaz dostarczania przez usługobiorcę treści o charakterze bezprawnym; 3) warunki zawierania i rozwiązywania umów o świadczenie usług drogą elektroniczną; 4) tryb postępowania reklamacyjnego. 4. Usługodawca świadczy usługi drogą elektroniczną zgodnie z regulaminem.	2) conditions for providing services by electronic means including: a) technical requirements necessary for co-operation with a teleinformation system, being used by the service provider, b) ban on delivering messages of illegal nature by a service recipient, 3) conditions for concluding and terminating contracts for providing services by electronic means, 4) procedure for making complaints. 4. Service provider renders services by electronic means according to the regulations.
Kodeks cywilny, artykuł 23: Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.	Polish Civil Code, Article 23: The personal interests of a human being, in particular health, freedom, dignity, freedom of conscience, name or pseudonym, image, privacy of correspondence, inviolability of home, and scientific, artistic, inventive or improvement achievements are protected by civil law, independently of protection under other regulations.
Kodeks cywilny, artykuł 24 §1: §1. Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.	Polish Civil Code, Article 24 par. 1: Par. 1. Any person whose personal interests are threatened by another person's actions may demand that the actions be ceased unless they are not unlawful. In the case of infringement he may also demand that the person committing the infringement perform the actions necessary to remove its effects, in particular that the person make a declaration of the appropriate form and substance. On the terms provided for in this Code, he may also demand monetary recompense or that an appropriate amount of money be paid to a specific public cause.
Kodeks cywilny, artykuł 471: Dłużnik obowiązany jest do naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi.	Polish Civil Code, Article 471: The debtor is obliged to compensate for damage resulting from non-performance or improper performance of the obligation, unless this non-performance or improper performance is a consequence of circumstances for which the debtor is not responsible.

Kodeks cywilny, artykuł 415: Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia.	Polish Civil Code, Article 415: Anyone who because of its own fault caused damage to another person is obliged to repair it.
Kodeks cywilny, artykuł 443: Okoliczność, że działanie lub zaniechanie, z którego szkoda wynikła, stanowiło niewykonanie lub nienależyte wykonanie istniejącego uprzednio zobowiązania, nie wyłącza roszczenia o naprawienie szkody z tytułu czynu niedozwolonego, chyba że z treści istniejącego uprzednio zobowiązania wynika co innego.	Polish Civil Code, Article 443: The circumstance that an action or omission which causes damage constitutes nonperformance or improper performance of an earlier obligation does not preclude a claim for remedy of damage based on tort unless something else follows from the substance of the earlier obligation.
Kodeks cywilny, artykuł 422: Za szkodę odpowiedzialny jest nie tylko ten, kto ją bezpośrednio wyrządził, lecz także ten, kto inną osobę do wyrządzenia szkody nakłonił albo był jej pomocny, jak również ten, kto świadomie skorzystał z wyrządzonej drugiemu szkody.	Polish Civil Code, Article 422: Liability for damage is borne not only by the direct perpetrator but also by any person who incites or aids another to cause damage and a person who knowingly takes advantage of damage caused to another person.
Prawo prasowe, artykuł 7 ustęp 2 punkt 1: 2. W rozumieniu ustawy: 1) prasa oznacza publikacje periodyczne, które nie tworzą zamkniętej, jednorodnej całości, ukazujące się nie rzadziej niż raz do roku, opatrzone stałym tytułem albo nazwą, numerem bieżącym i datą, a w szczególności: dzienniki i czasopisma, serwisy agencyjne, stałe przekazy teleksowe, biuletyny, programy radiowe i telewizyjne oraz kroniki filmowe; prasą są także wszelkie istniejące i powstające w wyniku postępu technicznego środki masowego przekazywania, w tym także rozgłośnie oraz tele- i radiowęzły zakładowe, upowszechniające publikacje periodyczne za pomocą druku, wizji, fonii lub innej techniki rozpowszechniania; prasa obejmuje również zespoły ludzi i poszczególne osoby zajmujące się działalnością dziennikarską.	Press Law Act, Article 7 Section 2 Subsection 1: 2. Within the meaning of this act: 1) press shall be considered periodical publications that do not constitute limitative and homogeneous entirety, are published at least once a year and bear a permanent title or a name, a number and a date, including, but not limited to: daily newspapers and magazines, newswires, telex messages, bulletins, radio and television broadcasts, film chronicles; press shall also be any means of mass media, existing and emerging in the course of technological advancement, including broadcasting stations and PA systems, that distribute periodical publications via print, video, audio, or any other broadcasting means; the press shall also cover teams of people and individuals engaging in journalistic activity.
Prawo prasowe, artykuł 50: Postępowanie w sprawach wynikających z niniejszej ustawy prowadzi się na zasadach	Press Law Act, Article 50: Proceedings in matters resulting from this Act are governed by the separate provisions unless otherwise provided herein.

określonych w odrębnych przepisach, chyba że ustawa stanowi inaczej.	
Prawo prasowe, artykuł 14: 1. Publikowanie lub rozpowszechnianie w inny sposób informacji utrwalonych za pomocą zapisów fonicznych i wizualnych wymaga zgody osób udzielających informacji. 3. Osoba udzielająca informacji może z ważnych powodów społecznych lub osobistych zastrzec termin i zakres jej opublikowania. 4. Udzielenia informacji nie można uzależniać, z zastrzeżeniem wynikającym z Article 14a, od sposobu jej skomentowania lub uzgodnienia tekstu wypowiedzi dziennikarskiej. 5. Dziennikarz nie może opublikować informacji, jeżeli osoba udzielająca jej zastrzegła to ze względu na tajemnicę zawodową. 6. Nie wolno bez zgody osoby zainteresowanej publikować informacji oraz danych dotyczących prywatnej sfery życia, chyba że wiąże się to bezpośrednio z działalnością publiczną danej osoby.	Press Law Act, Article 14: 1. Publishing or distributing audio or video information requires the consent of persons providing information. 3. A person providing information may stipulate extend and time of the publication due to substantial social reasons. 4. Providing information cannot be conditioned by, with exception of section 2, the fashion of comment or approval of journalistic expression. 5. A journalist cannot publish information if a person providing it stipulated it being subject to professional confidentiality. 6. It shall not be permissible to publish information and data on private life without consent of the person concerned, unless it is directly connected with public activity of such a person.
Ustawa z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych, artykuł 115 ust. 1: 1. Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.	Act of 4 February 1994 on Copyright and Related Rights, Article 115 Section 1: 1. Whoever usurps the authorship or misleads others as to the authorship of a whole or a part of another person's work or another person's artistic performance shall be liable to a fine, restriction of liberty or imprisonment for up to 3 years.
Ustawa z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych artykuł 116 ust. 1: 1. Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.	Act of 4 February 1994 on Copyright and Related Rights, Article 116 Section 1: 1. Whoever, without authorisation or against its terms and conditions, disseminates other persons' work, artistic performance, phonogram, videogram or broadcast in the original or derivative version shall be liable to a fine, restriction of liberty or imprisonment for up to 2 years.

Ustawa z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych artykuł 117 ust. 1: 1. Kto bez uprawnienia albo wbrew jego warunkom w celu rozpowszechnienia utrwala lub zwielokrotnia cudzy utwór w wersji oryginalnej lub w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.	Act of 4 February 1994 on Copyright and Related Rights, Article 117 Section 1: 1. Whoever fixes or reproduces other persons' work in its original versions or in the form of derivative version, artistic performance, phonogram, videogram or broadcast for the purposes of its dissemination and gives his/her consent to its dissemination without the authorisation or against the conditions specified therein, shall be liable to a fine, restriction of liberty or imprisonment for up to 2 years.

Bibliography

English titles

Legislation

Act of 6 September 2001 on access to public information;

Act of 21 February 2019 amending certain acts in connection with ensuring the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - General Data Protection Regulation;

Official Journal of the European Union: L 119/1;

Reports

Communication from the Commission to the European Parliament and the Council - Internet governance: the next steps / * COM / 2009/0277 final */

Case law

Yildirim v Turkey App. no 3111/10 (ECHR, 18 December 2012);

Delfi AS v Estonia App. no 64569/09 (ECHR, 10 October 2013)

Polish titles

Legislation

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r.;

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny;

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;

Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe;

Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny;

Ustawa z dnia 18 lipca 2002 r.o świadczeniu usług drogą elektroniczną;

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego;

Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi;

Decision of the President of the Office for Personal Data Protection of October 16, 2019, reference number: ZSPR.421.7.2019;

Decision of the President of the Office for Personal Data Protection of January 4, 2019, reference number: ZSPR.440.631.2018.

Reports

Szczepańska-Kulik I., Opinia do projektu ustawy o ochronie danych osobowych (druk sejmowy nr 2410), Biuro Analiz Sejmowych Kancelarii Sejmu

Books

Sobczak J., Swoboda wypowiedzi w orzecznictwie Trybunału Praw Człowieka w Strasburgu. Cz. 1, 'Ius Novum' 2007

Mrozek J., Rozważania prawne wokół pojęcia 'wolność słowa'; retrieved from URL: http://uwm.edu.pl/mkks/wp-content/uploads/11-cz-4-mrozek.pdf;

Wiśniewski A., Znaczenie wolności słowa w państwie demokratycznym 'Gdańskie Studia Prawnicze' 2000, no 7;

Olszyński M., Prawo Prasowe. Komentarz Praktyczny, LexisNexis 2013;

Chomiczewski W. Article 14. W: Komentarz do ustawy o świadczeniu usług drogą elektroniczną, [w:] Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw. LexisNexis, 2011;

Ogrodowczyk A., Żebrowska L., Murawska-Najmiec E., Twardowska K., Samoregulacja i współregulacja jako metoda rozwiązywania napięć w relacjach rynek-regulator, Warszawa 2018 r;

Podrecki P., Prawo Internetu;

Chałubińska-Jentkiewicz K., Article 14 [in:] Świadczenie usług drogą elektroniczną. Komentarz, 2019;

Nerka A., Article 17 [in:] red. M. Sakowska-Baryła, Ogólne rozporządzenie o ochronie danych osobowych. Komentarz;

Szczepaniak S., Article 7 [in:] red. M. Kawecki, Ustawa o ochronie danych osobowych. Komentarz;

Woiński M., Prawnokarne Aspekty Zwalczania Mowy Nienawiści, LexisNexis, 2014

Digital resources

<https://radcakancelaria.pl/2012/01/26/wolnosc-slowa-kilka-uwag-prawnych/> accessed 07 February 2020;

<https://iab.org.pl/> last accessed 12 February 2020;

<https://uodo.gov.pl/234> last accessed 30 January 2020;

<https://sjp.pwn.pl/sjp/wolnosc-slowa;2537413.html> accessed 28 January 2020;

<https://www.rpo.gov.pl/pl/kategoria-konstytucyjna/art-54-wolnosc-slowa> accessed 28 January 2020

Case law

Judgment of the Polish Supreme Court - Civil Chamber of 8 July 2011, reference number: IV CSK 665/10;

Judgment of the District Court in Warsaw of 14 August 2013, XX GC 757/12;

Judgment of the District Court in Szczecin of 4 August 2009, I C 764/08;

Judgment of the Supreme Court of 30 September 2016, I CSK 598/15;

Judgement of the Supreme Court of 8 February 2019, IV KK38/18;

Judgement of the Supreme Court of 8 February 2019, IV KK38/18;

Judgment of the Polish Supreme Court - Civil Chamber of 24 November 2017, reference number: I CSK 73/17;

Judgment of the Polish Supreme Court - Civil Chamber of 30 September 2016, reference number: I CSK 598/15.

ELSA Portugal

Contributors

National Coordinator

Rute Garrido

National Academic Coordinator

Alexandre Dias Pereira

National Researchers

Dussu Djabula

Francisco Arga e Lima

Inês Gamito

Joana Ferreira

Joel Alves

Juliana Pacheco

Mariana Baptista

National Linguistic Editor

Luciana Ayres de Campos

National Academic Supervisor

Alexandre Dias Pereira

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

1.1. How is Freedom of Expression protected in your national legislation

In Portugal, Freedom of Expression is a fundamental right, subject to the special regime of the so-called rights, freedoms and guarantees[1740]. It is expressly protected under the national Constitution, which establishes, under its Article 37, number 1, 1st half, that 'everyone has the right to express and disseminate their thoughts through words, images or any other means (…) without being subject to impediments or discriminations'.

Given its recognised importance for the autonomy and personality development of every human being,[1741] as well as for the proper functioning of the fundamental rights system as a whole and the democratic rule of law,[1742] most of the doctrine have been arguing that its normative scope should be interpreted as widely as possible[1743]. Thus, it should cover opinions, ideas, convictions, critics and value judgements about any matter, regardless of their purposes, evaluation criteria or even their truthfulness[1744]. It also should cover the right to silence[1745].

From a formal point of view, it encompasses 'the most diverse means suitable for the dissemination of thought'[1746], including oral or written words, images, posters, graffiti's, sign and body languages, television shows, movies, etc[1747]. It also embraces 'new types of expression, like 'blogs', 'chats' and 'electronic protests'[1748].

1740 About the specifics of that regime, see CANOTILHO, Gomes / MOREIRA, Vital, 'Constitution of the Portuguese Republic Annotated', Vol. I, 4th edition, Coimbra, Coimbra Editora, 2014, pp. 370 e ss.

1741 See ALEXANDRINO, José de Melo, 'O âmbito constitucionalmente protegido da liberdade de expressão', in 'Media, Direito e Democracia', 1st edition, Coimbra, Edições Almedina, 2014, page 48.

1742 See separate opinion of the judge MARIA LÚCIA AMARAL in the Decision 224/2010 of the Portuguese Constitutional Court, available in <http://www.tribunalconstitucional.pt>.

1743 See CANOTILHO, Gomes / MOREIRA, Vital, 'Constitution of the Portuguese Republic Annotated', page 572.

1744 Idem, ibidem.

1745 Idem, ibidem.

1746 See MACHADO, Jónatas, *apud* ALEXANDRINO, José de Melo, 'O âmbito...', page 52.

1747 See MIRANDA, Jorge / MEDEIROS, Rui, 'Constitution of the Portuguese Republic Annotated', Vol. I, Coimbra, Coimbra Editora, 2005, page 429.

1748 See CANOTILHO, Gomes / MOREIRA, Vital, 'Constitution of the Portuguese Republic Annotated' page 572.

1.2. Which legislation is in place to protect against limitation towards Freedom of Expression?

Article 37, number 2, of the Constitution of the Portuguese Republic, expressly determines that Freedom of Expression cannot be prevented or limited by any type or form of censorship. This means that not only the state or any other public powers, but also private actors (citizens, companies, etc.), are strictly prohibited to put in place any juridical or factual means intended or likely to restrict the exercise of this fundamental right[1749].

In this sense – and except for the restrictions that specifically apply to military and militarised agents[1750], as well as to the dissemination of information covered by secret duties[1751] – Freedom of Expression should, in principle, only be limited in the cases where it seems strictly necessary to ensure harmonisation with other legal and community interests and values such as the protection of morals, the right to privacy, etc[1752].

The violation of these limits (*v.g.*, through the practice of the crime of defamation) is subject to the general principles of criminal law or of the illicit of mere social order, being their appreciation respectively of the jurisdiction of the judicial tribunals or of the *Entidade Reguladora da Comunicação Social*[1753].

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

Currently, we live in a digital world and, consequently, there is an enormous amount of fundamental rights and freedoms that have been established for a long time which need special protection when facing new threats and challenges.

In Portugal, there is no specific legislation targeting blocking and taking down content of the internet. However, there is a legislation to, namely, punish criminals that commit crimes such as accessing or diffusing child pornography, defamation, online fraud, among other. Portuguese legislation also aims to protect constitutional rights and legal assets such as the rights of copyright, the

[1749] See CANOTILHO, Gomes / MOREIRA, Vital, 'Constitution of the Portuguese Republic Annotated', Vol. I, 4th edition, Coimbra, Coimbra Editora, 2014, pp. 574-575.
[1750] See Article 270 of the Constitution of the Portuguese Republic.
[1751] See, namely, Articles 20, number 3, and 164, paragraph *a)* of the Constitution of the Portuguese Republic
[1752] See CANOTILHO, Gomes / MOREIRA, Vital, 'Constitution of the Portuguese Republic Annotated', pp. 573-575.
[1753] See Article 37, number 3, of the Constitution of the Portuguese Republic

right of privacy and property rights, the right of self-determination (related to child pornography) and the right to honour and to a good name.

Despite of non-existence of specific legislation for this particular problem, there are some procedures in practical matters. It is now important to distinguish between 'law in books' and 'law in action': even if there is not a written law about a subject, ways to regulate an issue can always be found. In this case, for example, in Portugal, when a person lodges a criminal complaint about content on the internet that infringes their fundamental rights, asking as a provisional matter for the content to be taken down, the complaint will be presented to the public prosecutor who will eventually and after adequate appreciation of the complaint and its veracity, take the content down or block it.

Nevertheless, in the world that we live in now, most of the social media platforms already have mechanisms to report internet content and, therefore, to block it and/or take it down. There is a substantial amount of self-regulations that private entities apply to the users and to themselves on account of not having enough government legislation to cover every aspect on and related to internet content.

On this matter, Portugal is no exception and sometimes is very complacent with blocking and/or taking down internet content. An example of this situation was the time, in this case years, that it took for our country to takedown the hijacked websites (e.g.: torrents, pirate bay, etc.) when other European Union members had already done it.

Concerning legislation, all legislation about the internet and the security of the cyberspace is scattered over several different kinds of regulations. For example, Portugal has legislation related to this matter on the Constitution, criminal code, and copyright code. There are also many different bills such as the Law 109/2009, 15 September of 2009 (Cybercrime Law based on the Cybercrime Convention in Budapest – 23 November 2001), the Law 59/2019 (transposition of EU Directive 2016/680), the Law 144/99 (International Cooperation in Criminal Matters – 31 August 1999), the Law 58/2019 (8 August 2019 – executes the EU regulation 2016/679 on Data Protection of individuals related to personal data and free circulation of this data), the Law 50/2004, 24 August 2004 and, finally, the Law 46/2018, 13 August 2018 (transposing the EU Directive 2016/1148 – cyberspace security).

Moreover, Portuguese Cybercrime Office has, in fact, a considerable amount of cooperation with institutions such as Facebook, Microsoft, and Google, being the last one the most cooperative. The cooperation has its main focus on

collecting data to search for criminal activities. However, work is being done with the office in order to gather more information.

For now, no cases related to blocking and takedown of internet content where Portugal has been a party have been found yet. Nonetheless, research on this matter will be continued.

Nevertheless, it is known that Portugal does protect the right to honour and to a good name. An example of this situation is the ruling 671/14.0GAMCN.P1 where the publication of documents on Facebook with the intent of defamation is discussed. Although the decision wasn't totally in favour of the petitioner, this is a very important court ruling because it offered judicial protection to image and honour rights online.

Finally, the Government proposed in their state budget (approved by the Parliament this January) a project called the Digital Citizenship Charter. In this project, the creation of an entity is proposed. This entity has enforcement powers and mechanisms to ensure and protect fundamental rights that are put in jeopardy because of the users of the internet. In addition, the entity ensures the reinforcement of the democratic inspection over the internet and artificial intelligence. Lastly, it has the intention of controlling fake news and giving the citizens more accurate and verified information. Evidently, this can only work with an independent entity that has no ties with other organisations.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

3.1. Is content which is unlawful in civil law and content which is illegal under criminal law treated differently?

There are few specific provisions concerning internet content in civil and criminal law. On one hand, the protection of reputation and personal data is regulated in the Articles 79 and 80 of the Civil Code. The response of the civil law to unlawful content would be through civil liability, which has its general provision in Article 483, number 1 of the Civil Code. If a person saw the rights mentioned above violated, he/she would have the right to be compensated, in order to be put in the position where he/she would have been if the damage had not occurred.

On the other hand, criminal law regulates topics related to child pornography, found in Article 176 of the Criminal Code, counter-terrorism and national security, set by Law n.º 52/2003, of 22 August 2003, in its Articles 2, number 1,

paragraph c), and 4, numbers 2 and 5, and protection of reputation and personal data, present in Article 199 of the Criminal Code. The criminal law answers to these crimes with sanctions, which result in penalties of imprisonment or fines, varying according to the case in question.

Therefore, there is a clear difference, as civil law aims to apply civil liability in case of illegal content, whereas criminal law applies sanctions to those who disrespect the Law.

3.2. Does a content exist in your country under which otherwise legal content may be blocked/filtered or taken down/removed?

In Portugal, there are no provisions concerning the removal or blocking of legal content. The removal or blocking should only be justified if the content is illegal. It is clearly stated in Article 37, number 2 of the Constitution of the Portuguese Republic, that the exercise of Freedom of Expression cannot be stopped or limited by any kind of censorship. It is followed by numbers 3 and 4, where it becomes clear the only way to block or remove content is if an infraction has been committed in exercise of this right. With that said, no restriction of the right to Freedom of Expression can exist if the content is legal.

3.3. Which safeguards are in place to ensure a balance between censoring and Freedom of Expression?

Firstly, Freedom of Expression is regulated and can be found in Article 10, number 1, of the European Convention on Human Rights (ECHR), in Article 11 of the Charter of Fundamental Rights of the European Union, as well as in Article 37 of the Constitution of the Portuguese Republic.

Yet, limitations to this right are also stated in the referred Articles of the Criminal Code and the Civil Code, and in Article 10, number 2, of the ECHR. Furthermore, limitations can be equally found in the General Data Protection Regulation, as it aims to increase the protection of citizens' personal data.

There is a legal framework in place regulating both Freedom of Expression and its censorship. Nevertheless, the desired balance between both still does not exist, as the bottom line between the two remains unclear.

3.4. What is the process of judicial review of cases where content has been blocked or taken down from the internet? Which bodies conduct such review? Does the review constitute effective protection of Freedom of Expression online?

Normally, the judicial review of cases where content has been blocked or taken down from the internet does not differ from the process applicable to any other cases. The safeguards of the criminal process, present in Article 32, number 1, of the Constitution of the Portuguese Republic, include the possibility of review.

Firstly, the Article 209, number 1, of the Constitution of the Portuguese Republic, expresses that there are additional courts to the the Constitutional Court, these being the Supreme Court of Justice and the courts of first and second instance. The rule is that the case is judged in the first instance, with the possibility of it being reviewed in the second instance and having the Supreme Court of Justice on top of the hierarchy, according to Article 210 of the Constitution of the Portuguese Republic and Article 42 of the Law n.º 62/2013, 26 August 2013.

However, in case of administrative decisions led by bodies as the National Commission for Data Protection, there is the possibility of judicial review by administrative courts of first instance, as stated in Article 44 of the Law n.º 13/2002, of 19 February 2002.

Lastly, the process described above does not necessarily ensure an effective protection of Freedom of Expression online, as the lack of regulation necessarily influences the protection the process of judicial review may offer.

3.5. Does the legislation in your country on content filtering and takedown conform with requirements set out in the case law of the European Court of Human Rights? Please analyse the degree of compliance and explain where compliance is not reached as well as any reasons behind non-compliance.

There are two requirements set out by the case law of the European Court of Human Rights (ECtHR)[1754]. The first one is present on the case of *Ahmet Yildirim v. Turkey*,[1755] calling for a clear need of a legal basis while deciding any blocking measures, in order to prevent abuses.

The second requirement is present in the case of *Cengiz and Others v. Turkey*,[1756] concerning the needed quality of the law, as the legal system must delimitate its framework in respect to the blocking measures.

The requirements do not appear to be met, as there is little specific framework in place in order to regulate content filtering and taking down, simultaneously

[1754] Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content', 2017,014017GBR.

[1755] *Ahmet Yildirim v. Turkey* App no 3111/10, ECtHR, 18 December 2012.

[1756] *Cengiz and Others v. Turkey* App no 48226/10 and 14027/11, ECtHR, 01 December 2015.

with a lack of delimitation on the applicability of blocking measures. As most part of the legislation is vague and does not ultimately aim to regulate online content itself, the degree of compliance is, so far, low and not sufficient.

3.6. Include reference to and analysis of relevant case law. Please structure your case law analysis as follows: short outline of the facts, the decision and an evaluation of how the decision affected state of the law

Thus far, there is no relevant Portuguese case law on blocking or taking down internet content that has affected somehow the state of the law.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

As in other European States, Portuguese's internet access providers and website hosts have developed a lot of self-regulatory strategies, in order to compensate the void left by the legislator's choice not to intervene in the area at stake[1757].

A great example of that can be found in the recent signature of a memorandum of understanding between the General Inspection of Cultural Activities, the Association of Electronic Communications Operators, and three other associations representing producers, resellers and video authors, with a view to temporary blocking the illegal broadcasts of football matches of the national league on the Internet[1758].

A similar deal had already been signed in 2015, with the objective of blocking access to websites that were mainly dedicated to the unauthorised dissemination of works protected by intellectual property[1759].

1757 From a panoramic perspective of the subject, see European Council, 'Comparative study on blocking, filtering and take-down of illegal internet content', 2015, available in <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>.

1758 See 'IGAC, operadores e produtores de vídeo assinaram acordo para bloquear streamings piratas na própria hora', *in Exame Informática*, 18 January 2019, available in <https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2019-01-18-igac-operadores-e-produtores-de-video-assinaram-acordo-para-bloquear-streamings-piratas-na-propria-hora/>.

1759 See ROSA, Victor Castro, 'Memorando de Entendimento entre a APRITEL e as Entidades de Gestão Coletiva de Direitos de Autor e Direitos Conexos, sobre a proteção de direitos de propriedade intelectual na Internet', *in Propriedades Intelectuais*, 4, Universidade Católica Editora, November 2015, available in <https://dd.indie.host/uploads/default/original/1X/76978bf5e81258af8c17b49f1a80649d5f42e2f8.pdf>.

It is also very common for internet intermediaries to have terms of use policies that determine the blocking or take-down of contents considered offensive to the community standards[1760].

Generally speaking, that can be the case when contents involve nudity, explicit sex, or when they actively promote hate speech, violence, racism, xenophobia or any other type of discrimination[1761].

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

The Right to be Forgotten or the Right to Delete as enshrined in Article 17 of the General Data Protection Regulation allows the data subject to obtain from the data controller the elimination of his or her personal data. Albeit an important right that allows the data subject to control the information that is widespread, namely through social media and the internet, in Portugal it has not been the target of too much legislative and jurisprudential attention, especially in the context of the internet.

In fact, the main piece of legislation concerning the protection of one's data is Law n.º 58/2019, which implements specific provisions related to the execution of the General Data Protection Regulation. Here, it may be found that the Portuguese legislative body gave the power related to the deceased's personal data to the people designated by the deceased to that effect, or his heirs, as stated in Article 17 of that Law.

Moreover, in what concerns the publication of personal data in official journals, Article 25 states that even though the dissemination of personal data should respect the principle of finality and minimisation, the right to delete in this context is of an exceptional nature, being only given to the data subject if it is the only way to guarantee the Right to be Forgotten.

Another important piece of Portuguese legislation is Law n.º 59/2019 that approves certain rules concerning data processing in what relates to the prevention, detection and investigation of criminal infraction. Here, Article 17 states that the data subject is entitled to a Right of Erasure, without undue delay, if the data processing is not lawful, when it does not respect the general

[1760] By way of example, see Facebook community standards in <https://www.facebook.com/communitystandards/introduction>.
[1761] Idem, ibidem.

principles of data protection, or when such erasure is necessary in order to comply with a legal obligation.

With regards to the law in action, it must be mentioned that decisions made by the Portuguese courts related to this right have been, at the very least, scarce. In fact, the Portuguese courts (even the Constitutional Court) have dealt with cases related to video surveillance on working contexts, as well as tracing employees' browser search history, but they have never, at least directly, dealt with the Right to be Forgotten.

Thus, and concluding, Portugal did not adopt, up to this moment, a wide range of legislative actions in order to regulate the application of the Right to be Forgotten to specific contexts, namely the internet. The same may be seen when looking at the jurisprudential application of the right, where Portuguese courts have not dealt with this problem in a direct way.

6. How does your country regulate the liability of internet intermediaries?

In Portugal, the liability of internet intermediaries follows the same general standards as those imposed on other data controllers, without there being any specific national provisions regulating their activities.

Firstly, internet intermediaries are subject to the national provisions enshrined in Law n.º 58/2009. Nonetheless, this piece of legislation does not create any specific obligation for internet intermediaries to implement measures for blocking and taking down content, but only to proceed to the erasure of information when requested by the data subject (and if the request is deemed as legitimate), or when the objective of the data processing is accomplished, in accordance with Article 21 of Law n.º 58/2009.

On the other hand, Portuguese law takes into account the need to protect Freedom of Expression on broad terms and, as a consequence, in an online environment. The Constitution of the Portuguese Republic recognises Freedom of Expression as a fundamental right, as stated on Article 37. Furthermore, this right must be respected by data controllers when processing personal data. In fact, Article 24 of Law n.º 58/2019 states that data protection does not impair the exercise of Freedom of Expression, information and press, albeit in respect of human dignity and other fundamental rights enshrined in the Constitution of the Portuguese Republic.

Therefore, the Portuguese legal system demands a balance to be made between, on the one hand, Freedom of Expression and, on the other, right to privacy and data protection, as enshrined in Articles 26 and 35, respectively.

Thus, if a data subject considers that a data controller has limited his Freedom of Expression, Articles 32 and 34 of Law n.º 58/2019 allows him to turn to the National Data Protection Authority, Administrative and Judicial Courts.

Having this in mind, it can be concluded that Portuguese law does not regulate, in specific, the liability of internet intermediaries, but only subjects their activities to the general principles and provisions that deem data processing as lawful. Nonetheless, a considerable importance is given to the protection of the freedom of speech. This fundamental right must be protected by data controllers and, when the need arises, counter-balanced with the need to protect private life.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Article 37 of the Constitution of the Portuguese Republic establishes the Right to Freedom of Speech. This article undoubtedly and explicitly states that to exercise this right we shouldn't be censored. Having in mind the fact that the discussion around the blocking and the taking down of online content is essentially a discussion about freedom of speech, a fundamental right, we must try to foresee how in Portugal this discussion will develop.

To make this assessment one must take a look at the proposal of the new Directive on copyright in the Digital Single Market. The Directive, that still hasn't been transposed into national law, enforces that all digital platforms, such as Facebook and YouTube have to filter their information to prevent the usage and dissemination of content that's infringing copyrights. One of the articles that caused more controversy proposed the usage of effective technology which offers online services providers a way to recognise when content is a copyright infringement.

In a practical sense, this enforces filters on these online services that would clearly limit the Right of Freedom of Speech if the content that did not pass the filters couldn't be published. This example goes to show, or might be a foreshadowing of how the legislation regarding this topic will develop. Not only is it probable that new legislation will impose stricter policies on filtering online

content but internet intermediaries will also be held liable for not completely complying with legislation.

Additionally, to predict how the legislation will develop we can look at the Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to Member States on Internet freedom. Portugal, before passing new statutes into law, must conduct regular evaluations 'of the Internet freedom environment at the national level, with a view to ensuring that the necessary legal, economic and political conditions are in place for Internet freedom to exist and develop.'[1762] Those evaluations should be conducted by a legal entity such as the Ministry of Justice, or advocacy organisations that work together with the government. We must be careful not to paint this issue with a broad brush, which is one of the dangers we encounter.

Regarding the Right to be Forgotten, the development of that right has to be understood with the General Data Protection Regulation. This means that to analyse its implementation and future we have to look at how this particular regulation has been embraced.

The General Data Protection Regulation was an innovative and disruptive regulation that answered pressing issues of the modern world. However, due to the fact that this is a new regulation, it is implementation is still being studied and developed. The regulation raises many questions that haven't been answered at the rate we need. Specifically, when it comes to the Right to be Forgotten, it has been difficult to respond to the quantity of cases.

One example of this same issue is the fact that the National Committee for Data Protection stated, in 2019, that they had limited means to inspect and guarantee the proper implementation of the regulation. Also, in 2019, that same committee decided to 'unapply' nine articles of the law that enforces the General Data Protection Regulation in Portugal, namely concerning fines. The Commission concluded that certain rules of that law were manifestly incompatible with Union law.

This example is to show that even in five years the enforcement of the Right to be Forgotten and even of the regulation might not be in full force because of the difficulties that Portugal faces in order to correctly apply and transpose the regulation, which in turn will increase the response time to these types of cases.

[1762] Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom (Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers' Deputies) nº4

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

The internet expands the sphere in which we can practice our freedom of speech, which in turn has made our right to freedom of speech vulnerable. Hate speech is as dangerous offline as it is online, and in Portugal the balance between hate speech and freedom of speech in an online environment hasn't been reached.

Monitoring and filtering hate speech has become a greater challenge than expected. One issue faced by the country is the amount of content that is posted online with a hateful tone that cannot always be traced to the author, or, even if it could, the quantity of content online prevents a person from pursuing charges against every perpetrator.

To be able to allow for freedom of speech online and at the same time guarantee satisfactory protection to victims of hate speech online, we must answer the following question: who must be held liable when someone posts content online that is deemed hate speech?

Online service providers are mainly private companies and those same companies must provide ways to combat hate speech in its many forms. One way is for these services to establish rules and procedures that prohibit hate speech, but they must go even further and establish filters that in a reasonable way automatically prevent this type of content from even getting posted.

In the same way that online service providers must ensure the respect for copyright content, an economic interest, they will also have to ensure the takedown and blocking of hate speech, through these filters. The same mechanism for the assurance of copyright will have to be used to monitor hate speech, and companies will be held liable for the speech their users reiterate. This filtering technology raises issues regarding the protection of freedom of speech online. However, one thing to consider is that a speech is an act, and this act can endanger not only the person or group of people at which the speech is destined, but also society as a whole.

Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 10 of the ECHR protect freedom of speech, and as stated Article 37 of the Constitution of the Portuguese Republic also protects freedom of speech. Article 10 is quite important, since it establishes the conditions a government should comply with when imposing limitations on freedom of speech. Portugal

can limit freedom of speech 'for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others', which conveys more legitimacy to the mechanism of filtering.

Another step towards balance would be for the Portuguese legislation to convey a provision regarding the abusive exercise of fundamental rights, seen as this prohibition is a necessity to make it clear that inciting hate towards a person or a group of people cannot be justified as an exercise of the freedom of speech right.

Finally, the Law of Cybercrime nº 10972009 of 15 September 2009 should be reviewed and more provisions must be added. The law has to be much more specific, and should have provisions regarding hate crime and how we can combat it more efficiently online.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

Portugal hasn't reached an adequate balance between allowing Freedom of Expression online and protecting other rights, such as the Right to Information or the Right to Privacy. Besides, some laws present in Portuguese law seriously harm Freedom of Expression. Being Freedom of Expression one of the most important foundations of democracy, its efficient legislation and regulation are crucial. Leading with mis-, mal- and disinformation must be a priority in the current digital environment.

There is no breach in Portuguese jurisdiction concerning the Freedom of Expression regulation, as seen previously. Its application is what creates a problem. The principle of proportionality can be easily misapplied in a conflict of rights.

Concerning Freedom of Expression in general, there are several problems of efficiency in Portugal, considering it has an unusually elevated number of cases in the ECtHR for Freedom of Expression violations, established in Article 10 of the ECHR. For a long time, Portuguese courts did not distinguish between facts and opinions. It was the ECtHR that clarified that opinions aren't true or false. They vary from individual to individual and do not have to follow the opinion of the State or common sense.

The State opted for a judge's application of the existing laws, instead of developing new legislation or revising the current one. There should be a

National legislation scrutiny to include clear defence norms and define a reasonable limit for compensations, which should be proportional to the caused damage, as recommended by the International Press Institute. Furthermore, some rules of the Portuguese Criminal Code should be revoked, such as insult (Article 181), defamation (Article 180) and its penalty (Article 183), and criminal defamation of the deceased, which statute of limitations is 50 years (Article 185). Moreover, Article 184 states that when defamation or insult is committed against a wide range of government and public figures in virtue of their function, the minimum and maximum punishments are raised by one-half – this norm should be revoked or modified as it is clearly a violation to Freedom of Expression.

Only in these circumstances can we talk about a balance between rights: when there is a legal system that does not diminish the constitutional right of Freedom of Expression in order to criminalise defamation or insult.

Regarding the Right to Information, it is stipulated in the same article as the right to Freedom of Expression (Article 37 of the Constitution of the Portuguese Republic). This clearly shows how the two rights are connected and must be fulfilled in the same conditions.

The internet has indeed been a challenge to the consensus about Freedom of Expression. In its first years, the internet settled on the idea that everyone should have the opportunity to express their thoughts and everyone should have access to all content, including false content, with its evaluation and selection being the responsibility of each individual. However, practice has shown the fragility of this idea, since there is a lot of content propagating false information that can be harmful to people, such as unreliable material concerning health problems, misleading academic information or inaccurate political propaganda.

Information is impaired by Freedom of Expression if it isn't fairly regulated or if there are no effective ways to provide people the right information. There should be an investment in a reliable source of information for matters like the aforementioned. In that scenario, Freedom of Expression wouldn't be violated, nor would the right to accurate information.

10. How do you rank the access to freedom of expression online in your country?

On a scale from 1 to 5 concerning the access to Freedom of Expression online, I would rank Portugal with a 4.

Access to the internet is now materialised as a fundamental right of users (by the UN). In this digital space, there are also many other human rights, such as Freedom of Expression, thought, information and privacy.

The development of the media in the digital world has duplicated their space for sharing information, which allows people to be informed of almost everything, anywhere. Never has the right to Freedom of Expression and the right to information been more effective. However, risks have also grown and thorough legislation is more necessary than ever.

In Portugal, access to the internet is unlimited, as well as the right to freedom of speech. There is no sort of censorship applied to either of these rights and there are various ways to access the internet, such as in schools or public libraries.

Furthermore, there are no interdicted opinions. Each person can express their thoughts, without having to follow a certain 'truth' welcomed by the State. One can even criticise or question the values or principles of the Constitution of the Portuguese Republic. For example, even though torture is condemned in Portugal, one can manifest in favour towards that practice. Nevertheless, this easy access to Freedom of Expression can be impaired in a case of conflict of rights, as explained previously.

A certain opinion may be illicit if it offends other rights or interests. For example, the crime of discrimination and incitement to hate and violence (Article 240 Criminal Code), which consists of developing propaganda activities that incite or encourage racial, religious or sexual discrimination, among others. In those cases, Freedom of Expression must be blocked in order to maintain the State's security and democracy.

To conclude, Portugal is not far from an effective guarantee of Freedom of Expression, but there is plenty of work to do in order to reach number 5 on the scale.

11. How do you overall assess the legal situation in your country regarding internet censorship?

In the first instance, it should be noted that in the Portuguese legal system, the right to Freedom of Expression is constitutionally guaranteed in Article 37 of the Constitution of the Portuguese Republic. This being said, it should be emphasised that it acquires a wide scope of application, insofar as the possibilities of restricting it are extremely circumscribed, so that the rule that provides for Freedom of Expression 'without being subject to impediment or discrimination'[1763] has as little scope of application as possible. This broad interpretation of the rule is supported by Portuguese doctrine and jurisprudence, due to the concepts that focus on individual rights and freedoms, from which stems the right to the free development of the personality, as enshrined in Article 26, number 1 of the Constitution of the Portuguese Republic.

In this way, it is imperative to highlight that the practice of acts concerning the control and limitation of the right to Freedom of Expression is prohibited, regardless of whether the active subjects of the violation are public or private, subject to regulation by the Portuguese criminal law system. Situations are only exempted where legal assets of superior interest conflict with the right to Freedom of Expression and make the former prevail to the detriment of the second fundamental right, in situations where the legal value that is opposed over the Freedom of Expression, is superior as a legal asset.

In a more concrete approach to the issue of blocking and take-down of Internet content, the focus is on the lack of specific legislation on the subject. Reiteration will once again be placed on legislation punishing crimes relating to copyright infringement, industrial property rights, the right to honour and the right to self-determination.

Although they do not constitute a formally legislated and exhaustive list as content subject to withdrawal from the Internet, they represent an indirect route of punishment connected with the issue of blocking and removal of content from the Internet, making up a certain regulation of serious criminal offences, which would certainly be part of a specified legislation, if it existed. Because of this pressing need for regulation, private entities have strengthened means of self-regulation in order to restrict the possibilities of infringements by private users. However, it should be reinforced that the State Budget for 2020 provides for the establishment of an entity capable of guaranteeing fundamental rights that may be infringed by an abusive use of Internet functions.

[1763] Article 37, number 1 of the Constitution of the Portuguese Republic.

Nonetheless, it should also be noted that despite the scarcity of legislation, situations of illegality will be treated differently in civil law and criminal law. Consequently, they may be subject to civil liability, regulated under Article 483 of the Civil Code. In turn, Portuguese criminal law sanctions specific and determined offences with prison sentences or fines. However, given the lack of general regulation of the issue of content blocking on the Internet, there is still no relevant Portuguese jurisprudence on this matter.

Furthermore, although the General Data Protection Regulation provides in its Article 17 the Right to be Forgotten, i.e., the possibility of eliminating personal data, this right is scarcely regulated by Portuguese law, and, as a result, the possibilities of its protection seem limited to a situation in which the law of the Portuguese legal system is called upon to intervene in conflicts where protection of this right is specifically needed.

In conformity with the above, there is a need for intervention and reinforcement by the private sector with regards to the regulation of the takedown of content from the Internet. This necessarily stems from the misfortune left by the absence of national legislation in this regard. Thus, the urgency of the regulation of this situation by the competent national entities, specifically in invasive contents of the individual navigation sphere, is highlighted. These are generally self-regulated by private entities, and usually correspond to situations of sex, racism, discrimination, etc

From this indispensability of legislation linking the right to Freedom of Expression with the inevitability of a body of law legislating on the blocking of online content, the European Directive on Copyright in the Digital Single Market acquires primary relevance. It will allow the tracking of information that makes copyright infringements on digital platforms impossible. Despite being involved in controversy over the possibility of restricting the right to Freedom of Expression, it is in practice the most relevant regulatory instrument in force in Portugal regarding the blocking and elimination of online content in the coming years.

Moreover, the importance of the General Data Protection Regulation, which has been in force in its entirety since May 2018, is stressed by virtue of its regulation laying down the rules on the protection, processing and free movement of personal data of natural persons in all Member States of the European Union, in particular as regards the confidentiality of such data, their availability and non-adulteration. Despite the well-intentioned aims behind the creation of the Regulation, one cannot fail to stress the parsimony of means capable of guaranteeing the effective achievement of the purposes on which it is based.

As regards to the balance between the fundamental right to Freedom of Expression and its correlation with an imperative online hate speech, the same has not yet been achieved. This is precisely because of the lack of means to ensure control of hate speech. The most plausible solution for monitoring and consequently containing this discourse seems to be an automatic mechanism for eliminating content evaluated by a system of filters that prevent the release of offensive content. It is also noted that companies should be responsible for the hate speech that their users may adopt, so that a source of responsibility is reached, without absolving them from the task that binds them to the victims of the hate speech. However, this purpose will always have to be reasonably considered prior to the creation of these control mechanisms, since the broad normative conception that encompasses the right to Freedom of Expression is imperative to limit the creation and application of an abusive use of these means, and should be created for exceptional situations such as this, since it is offensive and violates the sphere of individual rights of the other.

In the digital sphere where this scope of Freedom of Expression is less restrained, the violation of individual rights by the force of this fundamental right proves to be colossal. Given the lack of regulation regarding the censorship of offensive content, the non-existence of a ban on publishing expressions, opinions and thoughts is notorious. It is in these borderline cases, in which legal assets of considerable value collide in comparison with the extent of Freedom of Expression, specifically situations of racial, religious or sexual discrimination, as was previously stated, that the exclusion of the legal asset from Freedom of Expression in relation to others is legitimised.

As is understandable, the right to Freedom of Expression is always and concomitantly at odds with other spheres of rights. The problem arises in a situation where for the conflict between the two dimensions of rights affecting the principle of proportionality, enshrined in Article 18 of the Constitution of the Portuguese Republic, must be used. This situation occurs when the boundary of decision by the interpreter-applicator is so tenuous that the principle is used in a shapeless way in similar situations.

Accordingly, the national legal system will only strike a balance between conflicting rights where, when balancing legal assets, the right to Freedom of Expression is not restricted by a legal asset of manifestly lower value. This situation arises from the misuse of the purposes for which Freedom of Expression has been used, namely the publication of erroneous, defamatory or misleading information. The inability to filter this information and to ensure the correctness of the information disseminated online that reaches the sphere of

private individuals is assumed to undermine a right to Freedom of Expression that is deprived of the characteristics that make it a fundamental right. Thus, it is concluded that there is an urgent need for mechanisms capable of segregating the information that is irradiated online, so that a balance is struck between the right to Freedom of Expression and the right to privacy of the personal sphere of the individual.

Conclusion

According to what was previously discussed, some concluding thought may be taken regarding Portugal's legislative efforts concerning internet censorship and Freedom of Expression.

First of all, any attempts of censuring information on the internet face the Constitution of the Portuguese Republic as a first barrier. In fact, Freedom of Expression is deemed as a fundamental right that encompasses a large scope of situations, namely those derived from the recent technological achievements, like social networks and other recent realities.

Nevertheless, Portugal still has a somewhat void legal space on what comes to ordinary law regulating internet censorship. In fact, the rules that exist aim mostly at tackling criminal activities or have at their origin the necessity of transposing International and European rules to the Portuguese legal system. Regarding civil law, the remedies that exist concerning internet censorship are mostly those that already existed prior to the technological advancements that we have felt over the past years, without many innovations concerning this new scenario. Therefore, Portugal still does not have specific legislation concerning the blocking or takedown of internet content.

The same may be said in terms of jurisprudence, or cases related to this topic, which are very scarce. Even though Portugal has regulatory authorities that analyse the legality of activities on the internet and has established contacts with the private sector in order to establish memorandums of understanding on what comes to the usage of the internet, there have not been many cases that have reached the courts.

That being said, and as a concluding remark, one might say that the general protection given to Freedom of Expression in Portugal is rather intense, stemming from the Constitution but also from ordinary law, notwithstanding the fact that the concrete balance between Freedom of Expression and the blocking of internet content still has some space to grow.

Table of legislation

Provision in Portuguese language	**Corresponding translation in English**
Constituição da República Portuguesa Artigo 20.º (Acesso ao direito e tutela jurisdicional efetiva) 3 – A lei define e assegura a adequada proteção do segredo de justiça.	Constitution of the Portuguese Republic Article 20 (Access to law and effective judicial protection) 3 – The law shall define and ensure adequate protection of the secrecy of legal proceedings.
Constituição da República Portuguesa Artigo 37.º (Liberdade de expressão e informação) 1 – Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações. 2 – O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura. 3 – As infrações cometidas no exercício destes direitos ficam submetidas aos princípios gerais de direito criminal ou do ilícito de mera ordenação social, sendo a sua apreciação respetivamente da competência dos tribunais judiciais ou de entidade administrativa independente, nos termos da lei. 4 – A todas as pessoas, singulares ou coletivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta e de retificação, bem como o direito a indemnização pelos danos sofridos.	Constitution of the Portuguese Republic Article 37 (Freedom of Expression and information) 1 - Everyone has the right to freely express and divulge their thoughts in words, images or by any other means, as well as the right to inform others, inform themselves and be informed without hindrance or discrimination. 2 - Exercise of these rights may not be hindered or limited by any type or form of censorship. 3 - Infractions committed in the exercise of these rights are subject to the general principles of the criminal law or the law governing administrative offences, and the competence to consider them shall pertain to the courts of law or an independent administrative entity respectively, as laid down by law. 4 - Every natural and legal person shall be equally and effectively ensured the right of reply and to make corrections, as well as the right to compensation for damages suffered.
Constituição da República Portuguesa Artigo 270.º (Restrições ao exercício de direitos) A lei pode estabelecer, na estrita medida das exigências próprias das respetivas funções, restrições ao exercício dos direitos de expressão, reunião, manifestação, associação e petição coletiva e à capacidade eleitoral passiva por militares e agentes militarizados	Constitution of the Portuguese Republic Article 270 (Restrictions on the exercise of rights) Strictly to the extent required by the specific demands of the respective functions, the law may establish restrictions on the exercise of the rights of expression, meeting, demonstration, association and collective petition by full-time military personnel and

dos quadros permanentes em serviço efetivo, bem como por agentes dos serviços e das forças de segurança e, no caso destas, a não admissão do direito à greve, mesmo quando reconhecido o direito de associação sindical.	militarised agents on active service and agents of the security services and forces, and on their legal capacity to stand for election. In the case of the security forces, even when their right to form trade unions is recognised, the law may preclude the right to strike.
Decreto-Lei n.º 47344/66, de 25 de Novembro (Código Civil)	Law Decree nr. 47344/66, of 25 November (Civil Code)
Decreto-Lei n.º 48/95, de 15 de Março (Código Penal)	Law Decree nr. 48/95, of 15 March (Criminal Code)
Lei n.º 13/2002, de 19 de Fevereiro	Law nr. 13/2002, of 19 February
Lei n.º 52/2003, de 22 de Agosto	Law nr. 52/2003, of 22 August
Lei n.º 62/2013, de 26 de Agosto	Law nr. 62/2013, 26 August
Lei n.º 58/2019, de 8 de agosto de 2019	Law nr. 58/2019, of the 8th August 2019
Lei n.º 59/2019, de 8 de agosto de 2019	Law nr. 59/2019, of the 8th August 2019

Bibliography

English titles

Legislation

Constitution of the Portuguese Republic

Charter of Fundamental Rights of the European Union

European Convention on Human Rights

General Data Protection Regulation

Reports

European Council, 'Comparative study on blocking, filtering and take-down of illegal internet content', 2015, available in <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>.

Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' (2017) 014017GBR

Books

CANOTILHO, Gomes / MOREIRA, Vital, **Constitution of the Portuguese Republic Annotated**, Vol. I, 4th edition, Coimbra, Coimbra Editora, 2014.

ALEXANDRINO, José de Melo, 'The constitutionally protected scope of Freedom of Expression', *in* **Media, Law e Democracy**, 1st edition, Coimbra, Almedina Editions, 2014.

MIRANDA, Jorge / MEDEIROS, Rui, **Portuguese Constitution Annotated**, Vol. I, Coimbra, Coimbra Editora, 2005.

Lei do cibercrime anotada por Pedro Dias Venâncio, Coimbra Editora, 2011, ISBN: 9789723219067

Periodicals

'IGAC, operators and video producers signed an agreement to block pirated streamings on the spot', *in Exame Informática*, 18th January 2019, available in <https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2019-01-18-igac-operadores-e-produtores-de-video-assinaram-acordo-para-bloquear-streamings-piratas-na-propria-hora/>.

ROSA, Victor Castro, 'Memorandum of understanding between APRITEL and the Entities for Collective Management of Copyright and Related Rights, regarding the protection of intellectual property rights on the internet', *in Propriedades Intelectuais*, 4, Catholic University Editions, November 2015, available in <https://dd.indie.host/uploads/default/original/1X/76978bf5e81258af8c17b49f1a80649d5f42e2f8.pdf>.

Digital resources

Facebook community standards in <https://www.facebook.com/communitystandards/introduction>.

Cnpd.pt

Programa do XXII Governo Constitucional 2019-2020 – https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=54f1146c-05ee-4f3a-be5c-b10f524d8cec

Dgsi.pt

Relatório da atividade do gabinete do Cibercrime Set. 2015-Dez. 2016 - http://www.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_anual_gabinete_cibercrime2015_02-03-2017.pdf

Case law

Decision 224/2010 of the Portuguese Constitutional Court, available in <http://www.tribunalconstitucional.pt>.

Ahmet Yildirim v. Turkey App no 3111/10 (ECHR, 18 December 2012)

Cengiz and Others v. Turkey App no 48226/10 and 14027/11 (ECHR, 01 December 2015)

Portuguese titles

Legislation

Constituição da República Portuguesa

Reports

Conselho da Europa, 'Comparative study on blocking, filtering and take-down of illegal internet content', 2015, disponível em <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>.

Books

CANOTILHO, Gomes / MOREIRA, Vital, **Constituição da República Portuguesa Anotada**, Vol. I, 4.ª Edição, Coimbra, Coimbra Editora, 2014

ALEXANDRINO, José de Melo, 'O âmbito constitucionalmente protegido da liberdade de expressão', *in* **Media, Direito e Democracia**, 1.ª Edição, Coimbra, Edições Almedina, 2014

MIRANDA, Jorge / MEDEIROS, Rui, **Constituição Portuguesa Anotada**, Vol. I, Coimbra, Coimbra Editora, 2005

Periodicals

'IGAC, operadores e produtores de vídeo assinaram acordo para bloquear streamings piratas na própria hora', *in Exame Informática*, 18th January 2019, disponível em <https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2019-01-18-igac-operadores-e-produtores-de-video-assinaram-acordo-para-bloquear-streamings-piratas-na-propria-hora/>.

ROSA, Victor Castro, 'Memorando de Entendimento entre a APRITEL e as Entidades de Gestão Coletiva de Direitos de Autor e Direitos Conexos, sobre a proteção de direitos de propriedade intelectual na Internet', *in Propriedades Intelectuais*, 4, Universidade Católica Editora, November 2015, disponível em <https://dd.indie.host/uploads/default/original/1X/76978bf5e81258af8c17b49f1a80649d5f42e2f8.pdf>

Digital resources

Padrões da comunidade Facebook
<https://www.facebook.com/communitystandards/introduction>

Case law

Acordão n.º 224/2010 do Tribunal Constitucional, de 2 de Junho de 2010, disponível em <http://www.tribunalconstitucional.pt>

ELSA Romania

Contributors

National Coordinator

Maga Răzvan

National Researchers

Adriana Bucurescu

Ioana Cotrău

Ileana Domnariu

Laura Foia

Iulia Mitrache

Andrei Păun

National Linguistic Editor

Pati Arsene

National Technical Editor

Andreea Luca

National Academic Supervisor

Alina Borlianu

Introduction

The objective of our report is to illustrate the concept of internet censorship as understood by our national legislation and put into practice by our national authorities.

One of our main objectives is to give an insight into the way Romanian authorities have understood to put into practice the GDPR Regulation. The implications of this are numerous and interesting from a multitude of points of view, given not only its inherent importance, but also the state of national legislation on the subject existent up to this point. The application of the GDPR Regulation has played a huge role in bringing a sense of order and coherence to this domain, which had not been very detailed within our legislation beforehand.

We have chosen to examine the concept of *censorship* in a concrete manner, observing its implications in the particular context of the pandemic crisis. In our opinion, this crisis has contributed a lot to our understanding of the notion of censorship, due to the fact that it proved censorship is not inherently bad. Despite its usual political negative implications, it can have positive objectives, and play an essential part in their achievement. Thus, it is essential that we separate a notion from the materialisation of said notion in given circumstances.

In the context of the global crisis caused by COVID-19, a lot of rumours and pieces of fake information, the so-called *fake news* have been made public. Therefore, it was essential for our authorities to take some measures in what concerns the process of filtering the information on this subject. Not only can these fake news lead to irresponsible behaviours, but they are also a very dangerous potential source of generalised panic. The most suggestive example of situations like this is represented by some fake social media accounts that claimed to belong to national authorities, which, on behalf of this, spread a lot of information that proved to be false in the end. Consequently, we can see how this can represent a danger for our national security, as it may well diminish the trust people have in the idea of authority and in the people representing it. There is, therefore, this fine line between the bad, opressive form of censorhip, on one hand, and the necessary, beneficial one, on the other, which aims at guarding a greater interest – the general interest.

Our report aims at presenting the overall situation of our national legislation on the issue of censorship, yet without claiming to be an exhaustive study.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

Censorship in Romania is considered, by some people, a delicate subject, given the fact that a communist government has ruled the country for about 40 years after the Second World War. Nowadays, the ban of censorship and the right to information (that also includes internet freedom) are considered fundamental principles of the Romanian democratic society.

As a member of the European Union, Romania also fulfils its international duties regarding human rights and applies any necessary regulations to ensure and protect the freedom of expression of its citizens.

Of course, the legislation uses the literal meaning of all of its terms to reduce the chance of misinterpretation. According to the Explanatory Dictionary of the Romanian language, the term *censorship* is defined as a control exercised upon the content of publications, radio and television shows and, in certain cases, mail and telephone conversations. It may also refer to an institution or body that exercises censorship[1764].

Because it refers to a fundamental democratic principle, censorship is mentioned firstly at a constitutional level. Thus, Article 30 of the Romanian Constitution regarding the freedom of expression clearly states that 'any censorship shall de prohibited' and that 'no publication shall be suppressed'[1765]. It is universally accepted that one essay is not enough to present the importance of the Constitution, given the fact that any other legislation act must respect the constitutional principles. In other words, censorship is, theoretically, undesirable and no other inferior act can surpass this principle.

It may also be reminded in other ordinary laws. For example, the Audiovisual Law no. 504/2002 determines the functioning of traditional mass-media (television, radio, newspapers). It ensures that no media institution may be oppressed, while also affording them full independence and responsibility over the broadcasted information.[1766]

On the other hand, mass-media is not completely free to present any kind of information, so a specific difference between censorship and control can be observed in the legislation. The Audiovisual Law offers a balance between the

[1764] Explanatory Dictionary of the romanian language, 2nd edition, Romanian Academy, Linguistics Institute, 2009

[1765] Constituţia României, Articolul 30

[1766] Law nr. 504 din 11 iulie 2002, publicată în Monitorul Oficial nr. 534 din 22 iulie 2002

independence of mass-media and the right to information of citizens (which are entitled to know the actual representation of reality), thus the actual control of these institutions is exercised using the documented truth, meaning that, for instance, a television programme, which during an informative (news-presenting) show presents or sustains false information, will be penalised according to the dispositions of the Audiovisual Law.

The institution in charge of fact-checking these media entities is the National Audiovisual Council which also functions according to Law no. 504/2002. Some of the content subjected to control may include protection of human dignity, the right to response or protection of minors. These principles are also mentioned, for example, in the New Civil Code. The NAC exercises its authority by applying different sanctions strictly after publication of said content, mostly pecuniary or public summons, but, like every other public authority, it does not have the possibility to censor or alter any activity of traditional media (such as prohibiting TV channels to broadcast a certain piece of information).

When it comes to internet censorship, the Romanian legislation maintains its principles of freedom. Thus, the information that people want to publish is not checked or altered beforehand. However, there are several regulations regarding the control of content that can lead to blocking and takedown from the internet after the respective information has been published. For example, Romania has adopted the General Data Protection Regulation as part of its international duties and established different non-patrimonial principles in the New Civil Code. We shall talk exhaustively about these measures in the next pages.

Another principle present in the Romanian Constitution that sustains the freedom of expression is the right to information.[1767]

In general, almost any form of content is or should be accessible to the citizens. As mentioned earlier, there are certain institutions (such as the National Audiovisual Council for traditional media) that ensure the people being able to reach out to correct information and that they can differentiate between facts and opinions. Also, the internet is open for almost any site in the world, being considered sometimes a reliable source of news.[1768]

However, not all content can be made public. The content subjected to exclusion from the right to information usually refers to matters of national security (information kept by secret services), information provided for on-going

[1767] Constituţia României, Articolul 31

[1768] CAPITAL, Alexandra Buican, 'The main sources of information for Romanian people' <https://www.capital.ro/principalele-surse-de-informare-pentru-romani-studiu.html>, accessed 31 May 2020

judiciary trials or investigations and the right to private/intimate life of people. In other words, the right to information is mainly limited in situations in which it clashes with other principles contained in the Constitution.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

One of the most important forms of *censorship*, of control over internet content, is represented by the way in which our personal data are handled. Censorship, generally, does not represent neither a necessary nor an acceptable set of measures to be taken in a democratic society. Yet, in exceptional cases, instead of violating the value of individual freedom and self-expression, it creates a safe context for it to be expressed in, as long as these measures are taken in determinate situations, for limited amounts of time.

One can see this even more precisely nowadays, in the context of a global crisis, which, as historian Y. Harari believes, *accelerates historical processes*[1769]. Thus, if it is generally important to protect our personal data no matter what the context is, it is actually essential for this data – and information in general – to be thoroughly controlled before and after it is available on the internet. This is due to the internet being a huge network, a potential stepping point for big social trends and phenomena – it can generate panic as well as it can help calm people down or help them protect themselves from fake news.

One of the most important pieces of Romanian legislation on the topic of protection of personal data is represented by the Law no. 190/2018 regarding the measures for the implementation of Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Another source of law on the issue is represented by the decisions of ANSPDCP (National Authority of Supervision of Personal Data Processing).

This regulation essentially emphasises the power that every individual has over the information concerning them that is shared on the Internet. We will therefore focus on internet users' rights regarding the takedown of inadequate, incorrect or in any other way undesired internet content centering around them. Another aspect that we ought to permanently keep in mind is the relation between EU law and national regulations, understanding the extent to which our

[1769] https://www.npr.org/2020/04/05/827582502/a-historian-looks-ahead-at-a-transformed-post-pandemic-world

legal norms have been updated as well as harmonised with regard to the European ones.

Above all, given that the act discussed here is a EU directive, its result is mandatory for the member-states, creating a more effective protection of personal data. An objective that is inherent to this one is also comprehending what personal data consists of, given that it is very possible that many people understood this notion much better from May 2018 on. The result of the directive is mandatory, but not the means of achieving said result, which remains part of the national competence of each and every state. In order to better understand the degree to which the directive has been applied in our country, not only theoretically, but also concretely, we should observe the practical measures that have been taken.

On one hand, many law firms have developed special GDPR packages for their clients, in order to help them understand if their rights regarding the protection of personal data are truly respected or not. Not only do they help them effectively and efficiently protect their rights, but they often offer the theoretical, conceptual basis on which GDPR ought to be understood. People need to be taught the importance of GDPR as well as what it virtually consists of. It is not only about defending one's rights, but also understanding what these rights refer to. This is why a rather *pedagogical* approach is so necessary sometimes, this is why customer packages that offer this kind of legal knowledge are so essential.

On the other hand, some authors that have been writing on the subject of the harmonisation of the EU's GDPR law within our national legal context have indicated a series of problems that have occurred in the process.[1770] One of the problems that one deals with most frequently is an excess of zeal that some authorities end up having because of their will to implement the regulations as well as possible. For example, the GDPR regulations are often implemented by means of a wrongful or incomplete process of informing the people they concern. The situation of CCTV cameras located in a mall is extremely common and suggestive as well – the simple act of placing a poster saying *'This area is under video-surveillance'* in the mall does not suffice, because it ought to be placed outside, before people actually enter the mall and it should offer them more information regarding what this surveillance implies (for example, the fact that it is conducted in order to maintain the highest level of safety for customers).

[1770] https://gdprcomplet.ro/cele-mai-frecvente-3-greseli-de-implementare-gdpr/

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

A high necessity of establishing a balance between the exercise of freedom of expression online and the protection of social interests and individual rights is acknowledged. Romanian legislation states that thoughts, opinions, beliefs and creations can be freely expressed and with regard to the means of expression, the constitutional provision refers to word of mouth, written means, images, sounds and other methods of public communication. Without expressly mentioning the online environment, the Romanian judicial and legislative practice has been constant in qualifying internet content as part of the public space.

The relevant constitutional provision can be found in Article 30 of the Romanian Constitution, which stipulates the prohibition of censorship and of publications' suppression. Said interdictions are conditioned by the respect of fundamental, constitutional rights, of strict interpretation and comprehensively mentioned in Article 30 (7) of the Romanian Constitution as follows: 'the defamation of the country and the nation, the urging of war of aggression, national, racial, class or religious hatred, incitement to discrimination, territorial separatism or public violence, as well as obscene manifestations, contrary to good morals, are prohibited by law.'

From a broader perspective, the provisions found in civil law and criminal law complete each other in order to best ensure a balance in the social environment and to better conform with the European and international requirements. Nevertheless, factual situations can fall under criminal law and occasionally under civil legislation. Primarily, infringements of limits to the freedom of expression online constitute criminal acts which are accordingly judged, the civil law element being oftentimes related to punitive damages.

Relevant legislation and case law can be found in matters referring to psychoactive substances, discrimination on grounds of race, ethnicity, child pornography, littering of justice, e-commerce, cyber-bullying. In the following paragraphs we will analyse legislations, decisions and their impact on Romanian state law.

Firstly, Law no. 194/2011 on combating operations with products likely to have psychoactive effects, other than those provided for by normative acts in force, indicates the appropriate measures to be taken by public authority representatives. Therefore, the Ministry for Communications and for the Informational Society is entitled to require providers of electronic

communications services to block the access to said sites' content provided that there is a risk of transactions involving psychoactive substances being made through electronic means. In said cases, a supervisory body has the obligation of notifying the Ministry in order to take the necessary actions needed to bring criminal activity to an end. This is a clear case of blocking illegal content online.

Secondly, a wider range of situations classify as discriminatory acts as a consequence of breaching the limits of freedom of expression online. As an example, we mention the Government Emergency Ordinance (GEO) no. 31/2002 on the prohibition of organisations, symbols and facts of fascist, legionary, racist or xenophobic character and of promoting the cult of persons guilty of committing genocide offenses against humanity and war crimes. Article 6 of this GEO qualifies as a felony the act of clearly denying, challenging, approving, justifying or minimising, by any means, in public, the Holocaust, genocide, crimes against humanity and war crimes, explicitly condemning the commission of these acts through information systems.

With regard to relevant case law, the process of judicial review can differ in accordance to the subject-matter of the case. In situations where discrimination is concerned, the first competent authority is the National Council for Combating Discrimination (NCCD). Its decisions can be challenged before the Court of Appeal, whose rulings are mandatory and final.

The factual situation subjected to judging before NCCD, found in Decision no. 60/2012, presents a public statement on the social media platform Facebook, addressed to protesters, in which a depreciative and contemptuous opinion was linked to the infamous slogan 'Arbeit macht frei'. The Council decided, therefore, that the issue referred to met the constituent elements of a discriminatory act, as it is described in Article 2 (1) and Article 15 of GEO no. 137/2000 on the prevention and sanctioning of all forms of discrimination. Before the Court of Appeal, the aforementioned ruling was reinforced, establishing that internet content can constitute a violation of fundamental rights, such as freedom of conscience and human dignity.

Thirdly, from an operational point of view, with regard to Article 374 of the Penal Code, regulating child pornography, it can be noticed that within the territorial structures of the Romanian Police regarding organised crime, there are cyber-crime departments established, which, besides the hacking or phishing offences, have competence in the matter of child pornography. These structures collaborate with the Directorate for Investigating Organized Crime and Terrorism and with the Romanian Intelligence Service to create a more efficient mechanism for taking responsibility, obtaining evidence, and identifying

offenders. It also has the competence to request the removal or blocking of internet content.

Furthermore, in the matter of e-commerce, the legislator intended and succeeded to establish a clear set of obligations for the service provider, thus regulating situations in which illegal activity might be conducted online. Therefore, Law no. 365/2002 states that 'service providers are obliged to interrupt, temporarily or permanently, the transmission on a communications network or the storage of information provided by a recipient of the service, in particular by eliminating or blocking access to it, access to a communications network or the provision of any another service of the information society, if these measures were ordered by the public authority'. The following article defines the public authority as primarily administrative authorities and, where appropriate, courts whose competence in the matter is established by the legal provisions in force, applicable in each case.

Lastly, with relation to cyber-bullying and hate speech online, the Romanian Supreme Court, in one of its decisions, classifies social media platforms as public space. During the criminal prosecution for an offence that can be circumscribed to the notion of hate speech, the prosecutor may request the competent court to order the hosting service provider to remove the information or to block access to it.

When analysing the compliance of national legislation with the European Convention of Human Rights and its associated guidelines, the conclusion reached is that Romania is situated on an ascendant trajectory towards a total conformity with said international documents. It can be said that the toughest problem Romanian legislation is facing is not the lack of legislative and judicial instruments to face internet challenges, but the rapid development of criminal activity online.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

When it comes to protecting fundamental rights, such as the freedom of expression, the principal sedes materiae is the Constitution of Romania. Thereby, freedom of expression of thoughts, opinions, beliefs, and freedom of any creation, by words, in writing, in pictures, by sounds or other means of communications in public are inviolable.[1771] Any censorship shall be

[1771] Constitution of Romania, Article 30 (1).

prohibited.[1772] However, the safeguards of the freedom of expression are not of an absolute nature, as Article 30 (6) states that freedom of expression shall not be prejudicial to the dignity, honour, privacy of a person, and to the right to one's own image.

In the private sector, the freedom of expression is regulated by the New Civil Code, the provisions of the Constitution being nuanced: the right of free expression, private life, dignity, one's own image; violations of privacy; limitations; presumption of consent; processing of personal data.

Addressing the issue of violating non-patrimonial rights, Article 253 of the NCC stipulates applicable sanctions. If the violation of non-patrimonial rights was undertaken using the right of free expression, the court can prohibit the illegal act (if it is imminent) or stop the violation (and prohibit it for the future, if it still lasts).

The court can also oblige the author of the illegal act to fulfill any measures considered necessary to restore the right (e.g. to publish the sentence of conviction).

The NCC does not make any express reference to the issue of blocking or taking down internet content. However, the special legislation does regulate sanctions such as blocking sites for failure of respecting certain legal obligations.

For instance, Article 7 of Law no. 196/2003 on the prevention and combatting of pornography stipulates interdictions and obligations for creators of pornographic sites (to password protect them, to establish a fee per minute of usage, to keep a clear record of the number of site visits). In case of receiving a notification and verifying the content of the site, the National Regulatory Authority for Communications and Information Technology asks the internet service providers to block access to the site in question.[1773] Non-compliance by the Internet service providers of the obligation to block access to sites that do not comply with the provisions of Article 7 constitutes a contravention.[1774]

Law no. 535/2004 on preventing and combating terrorism also states legal provisions on the blocking of sites that support terrorist activities or causes.

Since Romania is a member of the European Union, the provisions of Regulation 2016/697 become relevant in the context of blocking and taking down internet content.

[1772] Constitution of Romania, Article 30 (2).
[1773] Law no. 196/2003 on the prevention and combating of pornography, Article 14 (2).
[1774] Law no. 196/2003 on the prevention and combating of pornography, Article 14 (3).

For the provisions of Section 3 – Rectification and erasure – to be applied, the data subject shall notify the controller, the notice containing enough information for the right invoked (right to rectification, erasure, restriction of processing) to be exercised. The mechanism ensures communication between the data subject and the controller, allowing a non-contentious solution to the matter.

According to Article 17 paragraph 3, the right to erasure presents a set of limitations, such as the right of freedom of expression and information, or legal obligations which require processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in public interest or in the exercise of official authority vested in the controller.

Furthermore, the right to restriction of processing (Article 18) is limited by the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

The recipients of the personal data shall be informed of any rectification or erasure or restriction of processing unless this proves impossible or it involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.[1775]

In the context of the 2020 coronavirus pandemic, several Romanian sites have spread false information regarding the spread or even the existence of the virus. The National Agency for Regulation in Communications took the measure of closing them based on legal provisions enforced by Decrees of establishing and extending the state of emergency (Article 53 paragraph 3 of Decree no. 195/2020; Article 91 paragraph 3 of Annex no. 1 to Decree no. 240/2020.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

When examining the notion of the *right to be forgotten*, we should first understand the relative character of this right.

While always keeping in mind its importance, it is also essential that we do not see it as an absolute value and understand there may be variables and fluctuations in the way it is applied and protected.

[1775] Regulation (EU) 2016/679, article 19.

The relative character of this right has a natural correspondent in the temporary and exceptional character of the legal measures that are to be taken when these values are relativised – such measures are to be applied during well-determined periods of time (as clearly determined as they can be, given the concrete context – during the pandemic crisis, one cannot know when it is going to end for sure, but we can be optimistic enough to state it will end, thus the measures we take have to be clearly temporary). It is essential for the process of supervision to be bilateral – it is necessary that it is not solely people that are supervised by the state, but also the other way around.

The main source of Romanian law regarding the right to be forgotten/the right to delete/the right to erasure is represented by Article 17 of the GDPR, given that in our law system international treaties ratified by our Parliament are directly part of our internal law, as Article 11 (2) of the Romanian Constitution states. Unfortunately, our national legislation before the implementation of the GDPR did not have such a concept, which makes familiarising ourselves with it a little difficult. We only had legal norms that protected the processing of personal data as a whole, but not the exact concept of *the right to be forgotten,* which is a rather complex one, due to its moral and emotional resonance. The psychological comfort that one may experience while being told *you have the right to be forgotten*, you have *the right to be left alone* (we have encountered this concept, but, sadly, only within legal literature, not in the law itself), this comfort could help people assimilate the GDPR as a whole easier.

We should mention Article 77 of our Civil Code, which states that 'every processing of personal data, by automatic or non-automatic means, is to be made solely in the cases and within the conditions stated by the special law'. The special law the Code refers to is Law no. 677/2001 regarding the protection of persons concerning their personal data and the free circulation of this data.

Even though this law has been replaced by Law no.190/2018, it is interesting to see that we used to have legal norms on this issue within our national system as well, long before the emergence or implementation of the GDPR. Also, there are cases and situations in which that law is still in effect, so we should not ignore its existence.

The differences between these legal acts are still relevant, because they each reflect a different view on the issue of protection of personal data. It is then extremely interesting to see that Law no. 677/2001 does not mention *the protection of data*, but the *protection of persons*, which may well correspond to a clear separation that used to exist in people's minds between us and the information about us. Over time, given that the free circulation of data has become more and more

obvious, a more and more significant part of our lives, we realised that nowadays it is very difficult to separate ourselves from the information that is made public about us. The censorship of this information does not solely represent the censorship of some arid, objective, boring data, this censorship is a form of control we have over our image and reputation, over our personality. Understanding this difference shows not only the huge importance these pieces of information have, but also the degree to which we identify with them.

Therefore, the data subject has the right to obtain, from the controller, the erasure of personal data concerning them, and they are to obtain it without undue delay, provided that one of the situations mentioned in Article 17 applies to their particular case. The data may not be necessary anymore; the data subject may withdraw consent on which the processing is itself based, without any other legal grounds for the processing existing; the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); the erasure of the data may also be a consequence of the data having been unlawfully processed in the first place; the personal data may have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject or the personal data may have been collected in relation to the offer of information society services referred to in Article 8(1).

One very interesting legal case having taken place in our country, that illustrates vividly the concept of the right to be forgotten, is represented by the civil sentence no. 699/2020, pronounced by the Court in Pitești. In this case, the complainant asked certain links and URL addresses - posted by third parties - that are shown when one uses the search engine belonging to the defendant, to be revised. These links included content referring to certain criminal acts, content that the complainant asked to be removed, invoking the protection of the right to a private and family life as well as the GDPR. The motivation offered a detailed explanation of the right to be forgotten, arguing that the person to whom the data refers to is able to request the takedown of said personal data, if the data has been illegally processed/without the person's consent, or is no longer needed for the aims that is was necessary for initially. The defender also specifies that the right to be forgotten is not an absolute right, as the regulations allow the processing and keeping of personal data if this is necessary in order to protect the liberty of information and expression, when there is a general interest to protect. They also emphasise that in this case such a view cannot be held, because of the fact that the claimant had retired from their post as a prosecutor in 2008. The action was, however, rejected, because the defendant had no legal

standing in the matter, yet the case is extremely relevant due to the arguments the claimant brought before the court.

We believe students ought to be more profoundly familiarised with the notion of the right to be forgotten, because, if the liberty of speech, for example, is thoroughly studied in school, this concept is seen as a rather peculiar one. Understanding it and the GDPR as a whole better would contribute to comprehending the equilibrium between the protection of personal data and this liberty of expression way more in depth. The key is in always making the distinction between the private interest and the general one, as we have seen especially these last few months, when, being confronted with this pandemic crisis, we had to accept that some of our rights would be restricted for the greater good. The exercise of the right to information was restricted in order to allow the essence of this right to live on. Thus, the authorities competent to publish the statistics regarding the spread of the virus (the Ministry of Internal Affairs) were allowed to make these announcements only once a day, at a fixed time, 1 p.m. Not only did this limit the panic, but it also helped us focus on a unique and true source of information.

6. How does your country regulate the liability of internet intermediaries?

6.1 What is an internet intermediary?

An internet intermediary is an entity which provides services that enable people to use the internet. They include internet service providers, search engines and social media platforms. According to the Council of Europe, internet intermediaries play a very important role in our modern society. Their definition of the term refers to a service, which is constantly evolving and makes interaction on the internet between natural and legal persons easier. They play various roles, from connecting users to the internet and enabling processing of data, to gathering information and assisting the sale of goods and services. They are able to carry out several functions at the same time.

6.2 What is 'internet intermediary liability'?

Internet intermediary liability stands for the legal responsibility of intermediaries for illegal or harmful activities performed by users through their services. If the intermediaries are unable to fulfill their obligation of preventing the occurrence of unlawful or harmful activity by their users, the consequences might include

legal orders forcing the intermediary to act or expose the intermediary to civil or criminal legal action.

6.3 Does an obligation to implement the measures for blocking and taking down content exist?

Freedom of expression is essential to democracy. But with freedom, there are quite a lot of risks involved, such as sharing illegal content online or distributing fake information. Therefore, comes the need of implementing measures for blocking or even taking down content.

Article 10 of the European Convention on Human Rights states that everyone has the right to freedom of expression and access to information. This right applies equally offline and online and should be balanced with other legitimate rights and interests. Existing standards developed for traditional media may well apply to new media, which means they may be entitled to rights, but also subject to responsibilities.

For individuals to be able to enjoy freedom of expression and information online to the fullest, the Internet needs to be stable and open. Technical failures and intentional disruptions can impact access to information regardless of frontiers. The Council of Europe has developed a framework of international cooperation to prevent and respond to eventual disruptions of the Internet.

Frequently asked questions can be answered by simply informing ourselves.

For example, if one wants to know if they can ask a company to take down information they have previously shared, they can access the GDPR (General Data Protection Regulation) and it is explicitly written that a person has the right to ask for personal data, which is no longer of use, to be taken down by the company. This can occur when the information that one has shared with the company is no longer necessary or it was used illegally. Personal data that was shared when one was a child for example can be taken down at any moment.

This right is called 'the right to be forgotten'. In some situations, someone can ask the companies that made some personal data available to take them down. Those companies are also obligated to take reasonable measures and inform the others about taking down the personal information.

It is worth noticing that this right is not an absolute one, which means that other rights, such as freedom of expression and scientific research, are protected.

6.4 Are there any safeguards in place for ensuring the protection of freedom of expression online?

In principle, the notion of illegal content online seems easy to identify, because in theory, what is illegal offline is also illegal online.

In Romania, civil liability is regulated in the New Romanian Civil Code which constitutes the norm of common law regarding civil liability. From these norms of common law, in some specific fields, there are special norms and regimes, which have priority in application over the general law rule, which will be applied where there are no special regulations. The legal regime of civil liability of the company's service providers information was regulated through Law no. 365/2002 regarding electronic trade and articles 11-15 constitute the special norm. The Romanian law regarding electronic trade transposes the Electronic Commerce Directive into national law.

According to Romanian law any person has the obligation to respect the rules of conduct which the law or custom of the place imposes and should not prejudice, by his actions or inactions, the rights or legitimate interests of others. The one who acts with discernment and still fails to respect the law has to be held responsible for the damage they have caused. The general conditions for one to be held responsible for their actions are the existence of an illicit act of prejudice, of a causal relationship between the wrongful act and prejudice, and guilt. The liability of service providers can be engaged in any field, including copyright, industrial property, even pornography, human rights abuses and the list could go on. Romanian e-commerce law has established some exceptions from the general principle of liability of service providers (legal exemptions from liability), provided by Articles 12-15, when service providers are not held responsible for the information that is shared, stocked or facilitated

The exoneration of service liability is expressly and finitely provided by the law:

The first exemption concerns the liability of suppliers of a service provided by an informational society, acting as intermediaries through simple transmission ('Mere conduit'), regulated by Article 12 of the Romanian law of e-commerce. The article mentions that, if a service of an informational society deals with transmissions in a communications network, the information provided by a recipient of that service, or in ensuring access to a communications network, the provider of that service is not responsible for the information transmitted if some conditions are cumulatively met.

In this case of exemption from liability the service provider has to play a passive role, being only a channel for transmitting information for third parties, in which case they will not be held directly responsible, nor in solidarity.

The second exception is the exemption of liability of suppliers of informational society services that temporarily store information, storage coaching ('Caching'), regulated by Article 13 of the Romanian law of e-commerce.

According to this article, if an informational society service consists in transmitting information provided by a recipient of that service provider, through a communication network, that service provider is not responsible for automatic storing, intermediate and temporary transmission of the information transmitted, to the extent that this operation takes place solely in order to make the transmission of information more efficient to other recipients, at their request, if the conditions of the article are cumulatively met.

The third exception concerns suppliers of informational society services that permanently store information ('Hosting'), regulated by Article 14 of the Romanian law of e-commerce. According to this article, if a service in our society consists in storing the information provided by a recipient of that service provider, that service provider is not held responsible for the information stocked at the request of a recipient, if any of the conditions mentioned by the article are satisfied.

The provisions of the aforementioned articles should not be applied where the recipient acts under the authority or control of the service provider. These provisions should not affect the possibility of judicial authority or of requesting the service provider to cease or prevent the breach, and also may not affect the possibility of establishing procedures limiting or interrupting access to information. As it can be seen from the analysis of the legal provisions for exemption from liability listed above, in determining the existence and intensity of liability of participants in legal relations in the electronic environment, a maximum importance is given to the factors of knowledge of the information, of its control, being irrelevant if we are considering an editorial control or even a physical one in terms of information. While the directive exonerates the liability of service providers if the provider did not have the possibility to know the circumstances that lead to illegal information, the Romanian law provides that, for the exemption of liability in the case of damaging actions, the provider cannot have any knowledge about facts or circumstances that lead to the conclusion that the activity or information could harm the interests of a third party. This exception operates only when the provider does not have knowledge of either the fact that actions or information are illegally stocked or that the

activity or information could harm a third-party. This plays an important role, because, for a provider to be held responsible by the Romanian law, one has to prove that they had knowledge of the illegal facts.

After the analysis of the aforementioned articles, in determining the existence and intensity of liability for participants in legal relationships in the electronic environment, maximum importance is given to the factors of knowledge of the information, of its control, being irrelevant if we are considering an editorial control or even a physical one in terms of information.

The fourth exception is that of exoneration of liability for suppliers who provide information search tools and links to other web pages, regulated by Article 15 of the Romanian law of e-commerce.

According to this article, the provider of links and search tools that also facilitates the access to information offered by other providers, are not held responsible for that particular information, if any condition mentioned by the article is fulfilled.

The previous article does not apply if the recipient acts under the command of the service provider. This exception is not provided by the e-commerce Directive, it is particular to the Romanian legislation, but also to the legislations of other member states.

Another particularity of the Romanian legislation is the provision of Article16(3) of Law no. 365/2002, that states, as a general rule, that suppliers of services are obliged to interrupt, temporarily or permanently, the transmission in a communications network, or storing of information provided by a recipient of that service, in particular by removing information or blocking access to a communications network or the provision of any other service of an informational society, if these measures have been ordered by the public authority defined in Article 17 (2). One other particularity in our legislation is that the Romanian legislator did not transpose the possibility for a court or administrative authority to request service providers to prevent violations. That means that, at this moment, there is no legal base for compelling providers of services to install a filtration system of electronic communications in particular cases.

Concluding, in the Romanian legislation there is a special regulation which can be applied to the exemption of liability of service providers, which can be found in the Articles12-14 of the e-commerce Directive (Mere Conduit, Caching, Hosting) and adds two more: information search tools and links to other web-pages.

One other form of taking down inappropriate content, which can be applied in any state, not only in Romania, is simply reporting it. For instance, Instagram or Facebook provide this option, where one could report a photo of content that does not resonate with their interests and the social media sites can take them down in order for it not to be seen anymore by the people who were either offended by a post or simply thought it was not appropriate to share online.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Since Regulation 2016/679 was transposed into national law and became effective in the middle of 2018, it might take some time before jurisprudence and case law can reveal the legislative needs that are not entirely met by the new legislation.

Nonetheless, addressing the matter of online blocking and take down, liability of internet intermediaries and the right to be forgotten, it is clear that the legislators (both the European Parliament and the National Parliament) are acknowledging the digital reality.

The Internet makes dissemination of information so easily achievable that any legislator should take into consideration and try to find the right balance between fundamental rights and liberties such as the right to privacy (on the one hand) and the right to information or the liberty of expression (on the other hand).

As a suggestion, it might prove useful to emphasise the role of a non-contentious preliminary procedure for cases in which the interest that was violated is of a private nature. Such a measure, that mediates the interests of the parties, could lead to a relief of the courts.

Therefore, in order to keep the legislation in accordance with the real needs of the legal system, an important role will be held by doctrinaires and practitioners – who shall make their opinions and interpretations known through specialised studies, court decisions, preliminary decisions or appeals in the interest of the law.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

Aspiring to a well-defined democracy and a cohesive rule of law, Romania adheres to the international and, most importantly, European guidelines on its aim to strike the right balance between exercising and protecting the rights and liberties of its citizens. Therefore, the European Convention on Human Rights and the European Union Charter of Fundamental Rights find their application on the matter alongside national regulations.

Particularly, regarding the clash of freedom of expression and hate speech in the online environment, the primary aspect that needs to be dealt with is defining 'hate speech'. There is no unanimously accepted definition of this notion[1776], as both the Romanian legislator and the national doctrine appear to be reluctant to provide a comprehensive overview. The Government Ordinance (G.O.) no. 137/2000 regarding the prevention and sanctioning of all forms of discrimination lays down a reasonable, but indirect definition in Article 15, a legal provision aiming to sanction the offence of 'a behaviour affecting human dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment'. The addressee of such a message could be a person, a group of persons or a community belonging to a 'certain race, nationality, ethnicity, religion, social group or socially vulnerable category or due to their beliefs, gender or sexual orientation'[1777]. Therefore, this article was not necessarily designed to tackle the issue of 'hate-speech', but we believe that its content could cover the concept as it lists a wide range of criteria and consequences of an undesirable demeanor.

This kind of negative manifestation has existed long before the proliferation of the Virtual Era, but the nature of the Internet facilitated the overgrowth of hate speech, representing a conducive environment for transmitting and receiving information with more accessibility and visibility[1778]. As a consequence, hate speech appears to be a significant and direct drawback of the freedom of

---

1776 Hate-Speech in the Romanian Online Media, Radu M. Meza, Journal of Media Research, vol. 9 issue 3(26)/2016, <https://www.academia.edu/30173854/Hate_speech_in_the_Romanian_Online_Media>, accessed 18 May 2020, page 5

1777 The anti-discrimination Government Ordinance can be accessed in Romanian here: http://legislatie.just.ro/Public/DetaliiDocument/24129 (last accessed on 15.05.2020)

1778 Freedom of Expression and The Internet, Wolfgang Benedek and Matthias C. Kettemann, Council of Europe Publishing, 2013, page 83-85

expression online that needs to be tackled with through carefully tailored policies and their effective enforcement.

In Romania, the legal framework is described as comprehensive, ensuring adequate protection and remedies to the individuals whose human dignity or private life has been violated[1779]. The legal safeguards are embedded in both civil and penal law, deriving their source from constitutional and European rules. As stated in the ECHR as well as in the EU Charter, the freedom of expression is not an absolute right and national authorities are allowed to interfere under rigorous conditions[1780], Romania making use of these provisions in its national law.

The Romanian Constitution. revised in 2003, provides in Article 30 (6) that 'Freedom of expression shall not be prejudicial to the dignity, honour, privacy of a person, and to the right to one's own image.', while in paragraph (7) it prohibits '(…) any instigation to national, racial, class or religious hatred, any incitement to discrimination (…)'. Therefore, it is revealed right from the first and of utmost importance source of law in our country that there is a high interest in providing protection against hate-speech in any area or environment.

Furthermore, substantial legal provisions are comprised in the Civil Code enforced on the 1st of October 2011, especially throughout the section with regard to respect to private life and human dignity[1781]. Thereby, the Romanian legislator is concerned with ensuring a wider framework, including under its guard the dignity of individuals even after their death, the legal action being introduced by their heirs[1782].

Moreover, Article 253 provides for concrete remedies and measures of protection to be taken by the judicial system: prohibiting the commission of the tort, if it is imminent; ceasing the interference and prohibiting it for the future; stating its illicit character, if the disturbance it has caused still persists; publishing the judgement on the expense of the perpetrator; any other compensation.

1779 Freedom of speech in the Romanian legislation, Diana Olivia Hatneanu, Centrul pentru Jurnalism Independent, 2013, < http://cji.ro/wp-content/uploads/2020/04/13.-Libertatea-de-exprimare-in-legislatia-romaneasca-Final-2.pdf >, accessed 18 May 2020

1780 The European Convention of Human Rights, Article 10 (2) and the European Union Charter of Fundamental Rights, Article.11 and Article 52.

1781 Notably, freedom of expression (Article 70), right to private life (Article 71), right to dignity (Article 72), right to own imagine (Article 73), interferences to private life (Article 74), limits(Article 75), respect to the deceased person (Article 78), prohibition to interfere with a deceased person's memory(Article 79), protecting human personality (Article 252), means of protection are the most relevant in this context (Article 253).

1782 Romanian Civil Code, Article 256.

However, there is one noteworthy exception: when the interference is caused by exercising the freedom of expression, the first measure, more specifically 'prohibiting the commission of the tort, if it is imminent' cannot be applied. This is due to the fact that it could be regarded as a form of dissimulated censorship, but the legal doctrine appreciates this rule as excessive and unreasonable as it should be enforceable with regard to vulnerable individuals, mainly minors and people with disabilities[1783]. We share this opinion as these legal measures, as good as they may appear to be on paper, need to prove themselves as practical, genuine tools to those who seek protection and that may be suffering from a substantial breach in their right to dignity.

By contrast, in the field of criminal law, there has been a consistent makeover since the enforcement of the New Penal Code in 2014. Before this moment, the legislator from 1968 condemned the crime of insult (Article 205) as an 'interference to honour or reputation through words, gestures or any other means, or exposure to mockery', whereas calumny (Article 206) was described as 'affirming or imputing in public, by any means, a determined deed regarding a certain person, which, if it were true, it would expose that person to (…) public contempt'.

Even though these provisions are no longer into effect, these articles are worth mentioning as, after the legislator repealed them in 2006, the Constitutional Court ruled through a judicial review that, by decriminalising these felonies, there would be a 'void in regulation'[1784]. Therefore, it caused an unacceptable failure to secure an effective protection of human dignity as civil remedies are clearly not sufficient to stand alone as practical safeguards, hindering individuals even from exercising their right to access to a court.

The legislator did not abandon its policy and, through the New Criminal Code from 2014, it decriminalised them again, but it slightly modified the crime of incitement to hate or discrimination (Article 369) so as to serve as a replacement. The lack of reaction from the Constitutional Court or other public authorities reflects the real (dis)interest in truly regulating this area. *De lege ferenda*, acts of discrimination and hate-speech must be considered as crimes when a minimal threshold is crossed, especially since the growth of the Internet. The online environment facilitates us to convey a message to a wider group of people or geographical area, with no boundaries. Insult and calumny, as described in the former Penal Code, are more likely to find their applicability in this context

[1783] Introduction to Civil Law, Ionel Reghini, Serban Diaconescu, Paul Vasilescu, Ed. Hamangiu, 2013, page 360.
[1784] Decision no. 62/2007 of the Constitutional Court of Romania.

rather than in the period before the 'boom' of the Internet and social networks in our country.

In practice, the Romanian case law for civil and, more preeminent, penal proceedings, indicates a scarcity in the field of online protection, even though these two would be the most effective and should have a more proactive approach. Arguably, this underlines a policy of non-intervention for this particular fact as, despite all the efforts to regulate this matter, the prosecution established a really high threshold to consider 'hate-speech' a crime and not a contravention[1785]. Certain considerations of the prosecutors to cease criminal proceedings were that 'hate-speech' must possess a large scale and consistency so as to create a genuine risk, to seriously affect social relationships, often arguing that hate messages were more likely simply critical opinions respecting the freedom of speech[1786]. We highly criticise this approach as it overthrows any efficiency of the provisions previously mentioned and inserts additional requirements that have no legal basis.

Nevertheless, to complete the legal framework, special legal norms have been adopted : the aforementioned Government Ordinance (G.O.) no. 137/2000 regarding the prevention and sanctioning of all forms of discrimination; Government Emergency Ordinance (G.E.O.) no. 31/2002 regarding the prohibition of organisations, symbols and acts with fascist, legionary, racist or xenophobic character and promoting the cult of personalities condemned of committing felonies of genocide, crimes against humanity and war crimes; Ordinary Law no.504/2002 of the audio-visual communication[1787].

G.O. no. 137/2000 of anti-discrimination established the ground rules for the functioning of the National Council for Combating Discrimination (CNCD), a state authority designed to prevent, investigate, monitor and sanction discrimination as well as providing assistance to those discriminated. We can define this public authority as a 'gate-keeper'[1788], analysing the context and content of the information conveyed by any means accessible to the public,

---

1785 The latter is under the competence of an administrative body, the National Council for Combating Discrimination, described two paragraphs further.

1786 A comparative analysis over the legislation and case law in the field of discriminatory or hate speech, Iustina Ionescu, Adriana Iordache, research realised with the support of Open Society Foundations (OSF), Think Tank Fund and Roma Initiatives Office, September 2015, available here, page 16-18

1787 In the same order, the sources in Romanian of these regulations are:
http://legislatie.just.ro/Public/DetaliiDocument/24129,
http://legislatie.just.ro/Public/DetaliiDocument/34759,
http://legislatie.just.ro/Public/DetaliiDocument/37503 (last accessed on 12.05.2020)

1788 Freedom of speech in the Romanian legislation, Diana Olivia Hatneanu, Centrul pentru Jurnalism Independent, 2013, < http://cji.ro/wp-content/uploads/2020/04/13.-Libertatea-de-exprimare-in-legislatia-romaneasca-Final-2.pdf >, accessed 18 May 2020, page 7.

including the online environment. It is an intermediary between individuals and the State, guardian of proper functioning of the legal rules, providing legal instruments for the individuals to exercise their rights and to seek compensation when they are infringed. As a consequence, it takes up the role of arbitrator and educator of a society in need of guidance to filter the information they emit and receive.

By far, this institution presents itself as the most active one with regard to hate-speech. After analysing their individual decisions[1789] and consulting reports on their activity from 2016 to 2018[17901791], we can conclude that the Romanian community has a strong connection with its own national history and values, proving an unfortunate lack of tolerance. Hence, the Rroma people, the Hungarians requesting autonomy or the Germans in Transylvania, atheists or the LGBT community have been affected by different forms of discrimination and hate speech in Romania, a rather conservatory country dominated by orthodox Christians, attached to their own traditions and language. Moreover, not only the addressees of hate-speech are important, but also the issuers: among persons with no special position, there are politicians posting on their own Facebook page or journalists publishing on news websites with a very high reach and ratings.

The Council represents an actor which was somehow delegated with the duty of sanctioning 'hate-speech'. It has been an active presence for the last few years and, as a consequence, the jurisprudence is mostly rich in administrative cases against which perpetrators seek to override its decisions. Nevertheless, our assessment revealed that its activity is not necessarily equivalent to its effectiveness. The National Council for Combating Discrimination is entitled to give fines as its most severe sanction, measure that proves as having little impact on educating and redressing the society, in general, and the perpetrator, in particular. As an administrative body and under political servility, this institution does not possess the adequate means to ensure the proper bridging between theory and practice.

The online is a dynamic environment that requires an increased attention to every instance and cannot be handled in a shallow manner. As a topical example, the COVID-19 crisis reignited animosities in the Romanian society, serving as

1789 CNCD, <https://cncd.ro/discriminare>, accessed on 25 April 2020.

1790 ActiveWatch, 'Annual Report on Intolerant Discourse and Hate Speech, 2018' <https://activewatch.ro/Assets/Upload/files/Raport_ActiveWatch_Hate_Speech_2018.pdf>, accessed on 29 April 2020.

1791 ActiveWatch, 'Annual Report on Intolerant Discourse and Hate Speech, 2018' <https://activewatch.ro/Assets/Upload/files/00_Raport%20hate%20speech_final%20(1).pdf>, accessed on 29 April 2020.

evidence of deeply rooted discriminations and misconceptions: from politicians expressing their views on their personal Facebook page on the Rroma people as vectors of spreading the virus, to extreme vilification of the Orthodox Church as it was not willing to respect the lockdown measures for the Holy Resurrection night[1792]. The president of CNCD captured these disappointing opinions in a brief evocative statement: 'Hate exploded in the public space. Especially online.' and declared the institution will look into it, while we remain skeptical.

By highlighting the most important laws and regulations on the matter of discrimination and freedom of speech, one can observe that the Romanian legislator has been eager to transpose the international guidelines into national legislation. Overall, these regulations strengthen the idea of the unavoidable 'but' when it comes to one's freedom of expression[1793], as it entails a number of limitations and permanent supervision so as to avoid any interference with others' right to human dignity or private life amounted in hate speech. The Romanian legislator has adopted the recommendations and directing principles with regard to striking the right balance between these two concepts and, as a result, the legal framework appears to be suitable for maintaining this mechanism. As praiseworthy as it may seem, there still remains the issue of effectively implementing these measures and Romania has not passed this exam with flying colours.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

We have previously mentioned different ways and institutions in which there is a certain control exercised upon public information.

As John B. Finch said, 'Your right to swing your arm leaves off where my right not to have my nose struck begins'. The same principle can be found in romanian legislation, which sets a few clear boundaries for the freedom of expression, more precisely one's freedom of expression should not bring any prejudice to another's non-patrimonial rights. In this case, the New Civil Code dedicates

[1792] Digi24, Alexandru Costea, 'Explosion of hate in the public sphere' <https://www.digi24.ro/stiri/actualitate/politica/a-explodat-ura-in-spatiul-public-cncd-analizeaza-un-val-de-plangeri-pentru-rasism-atacuri-la-bor-si-discriminarea-catolicilor-1293558>, accessed on 2 May 2020

[1793] Information Disorder - Toward an interdisciplinary framework for research and policymaking, Claire Wardle, PhD and Hossein Derakhshan, Council of Europe, October 2017, page 73

Book I, Title V to 'Defending of non-patrimonial rights', offering the prejudiced person a way to protect its own image, dignity, honour or privacy.

Even more, the Constitution explicitly states activity against the population, either against the majority or minorities, or against the country itself (instigation to war, hatred, discrimination, terrorism or obscene conduct) is strictly forbidden.

There are also certain cases in which freedom of expression may be profoundly limited if necessary.[1794] For example, because of the pandemic of 2020, the president of Romania has proclaimed a state of emergency with the purpose of slowing down the spreading of coronavirus. In this state, local authorities have slightly enhanced powers and may adopt certain regulations in order to protect the population. Because it is a matter of national security and public health, it is extremely important to inform the citizens correctly. Thus, any source that presents an uninformed statement or without scientific evidence can be taken down more easily strictly because of the newly created legislative environment.

10. How do you rank the access to freedom of expression online in your country?

Freedom of expression is the ability someone has to express their beliefs, ideas or opinions in a safe environment while respecting the law and the restrictions regarding this subject.

According to Article 70 of the New Romanian Civil Code, any person has the right to freedom of expression and this right can only be restricted within the limits provided by the law. Article 75 says that it does not constitute an infringement provided in this section, the violations permitted by law or by the international conventions and treaties regarding human rights to which Romania is a party. The same article explains that exercising our rights with good faith by respecting our Constitution and the pacts and international conventions to which Romania is a party does not constitute a violation of the articles provided in this section.

We can conclude that our law allows freedom of expression, but it can only be exercised within the limits provided by it. It is essential for a democratic society to respect pluralism, which implies not only political pluralism, but also the possibility to put into motion, with any help available, ideas.

[1794] Constituţia României, Articolul 53

Article 30 of our Constitution provides a large palette of rights and restrictions regarding freedom of expression. For example, it explains that freedom of expression cannot be censored in any way and that the civil liability for the information or the creation that has become public and known by the others returns to the creator of this content.

It is undeniable that freedom of expression is restricted in many ways and if someone is either offended by a piece of content or finds it disturbing or disrespectful, he/she has the right to contact the creator of that content directly. It is believed that this could be helpful for the creator to have an insight on what they choose to share and to perceive what should or should not be shared with the public.

The European Convention on Human Rights clarifies, in Article 10, that anyone has the right to freedom of expression. One can express themselves freely without taking into account frontiers, but the state can limit this right by establishing some limits in fields such as radio or television so that content which may not be appropriate for the public eye will not be shared.

GDPR (General Data Protection Regulation) is a regulation about the conditions under which a company can collect personal data, with one's consent, that is then shared online. It establishes some ground rules for all the departments of a company. This can assure internet users that their information is not used against them and that they can share it in a safe environment.

As for the exercise of freedom of expression in the online environment, indeed, without distinction, it is guaranteed, yet it is nevertheless subject to constitutional limitations. The explanation resides in the Article 30 (1), according to which the means of communication (the channel of speech) does not represent a hindrance in the exercise of the freedom of expression.

In this regard, the European Parliament and the Council of the European Union adopted Decision no. 276/1999 / EC on the 25th of January 1999 amended by Decision no. 1151/2003 / EC on the 16th of June 2003 introducing the notion of self-regulation, as the way of controlling online content through filtering and rating tools. Moreover, by means of these community normative acts it is encouraged to inform teachers and parents about Internet usage, them being the only ones able to agree on the use of filters meant to protect the children. As for the latter, educating them on how the Internet works is essential.

Some people have expressed their opinions regarding freedom of expression during the lockdown that has been implemented because of the pandemic we are all going through. Two lawyers from a law firm in Bucharest have expressed

their viewpoints on what rights have been restricted during this period of time and whether they have been founded or not. In their opinion, the fact that everything has been 'moved' online offers individuals the possibility to spread fake news, which can lead to panic among others. This panic can lead to all sorts of social movements that could have greater destructive effects than the crisis itself, which has facilitated the dissemination of that information. An example would be a document that was sent at the beginning of the quarantine on multiple WhatsApp groups that explained the restrictions which are going to be implemented in our country. It turned out that it was just a draft and the source was not a reliable one. That draft has created a lot of damage among others because not only has it caused panic to some people, but the authorities had to take action and explain that the document is not real and that everyone should wait until the government shares information which is supposed to be true and reliable.

In accordance with Article 54 of Decree no. 195/2020, the National Authority for Administration and Regulation in Communications ('NAARC') may order a series of measures to block information that promotes 'false news about the evolution of COVID-19 and protection measures and prevention'. In this regard, Decree no. 195/2020 requires that the removal of content be done 'at source', by hosting service providers and content providers, and if the removal at source is not feasible, NAARC may order network providers to immediately block access to that content.

In the current context it is essential for the citizens to be informed about all the risks they are subject to, and all the obligations they have to follow in order to stay safe and not be affected by the virus. Accurate information is essential for managing the crisis situation, and the efforts of the authorities, responsible journalists and civil society must be appreciated. However, the concrete measures that could be taken under Article 54 of Decree no.195/2020 raised some questions, in particular due to the ambiguity of the notion 'false news about the evolution of COVID-19 and protection and prevention measures', reaching opinions in the sense that it could lead to the establishment of a censorship mechanism.

The establishment of the state of emergency pursuant to Article 93 of the Romanian Constitution allows public institutions and authorities (mostly the state) to take certain extraordinary measures, but only in strict compliance with the constitutional provisions and the provisions contained in the Government Emergency Ordinance no. 1/1999 on the state of siege and the state of emergency ('GEO no. 1/1999'). Democracy cannot be restricted and the

freedom of expression cannot be bypassed. However, fundamental rights and the exercise of some rights can be restricted only by respecting Article 53 of our Constitution and Article 3 (8) from GEO no. 1/1999, that mention the fact that the state of emergency can only be established in compliance with the obligations assumed by Romania according to international law.

Any restriction on freedom of expression must be necessary in a democratic society and the measure that is taken must be proportional to the situation which led to it. Even international instruments on the protection of fundamental rights allow the Romanian state to impose certain restrictions on freedom of expression, when such measures are necessary, for example, for the defense of public safety or the protection of health.

The application of restrictions on freedom of expression - in order to ensure the correct information is provided to the population in the context of the crisis caused by the COVID-19 epidemic - meets only one of the conditions that must be met cumulatively in order to restrict the exercise of freedom of expression. The purpose pursued is as legitimate as possible. However, it will be necessary to analyse, on a case-by-case basis, whether a concrete measure that is to be ordered based on Article 54 of Decree no. 195/2020 is necessary and proportional in a democratic society.

From this last perspective, Decree no. 195/2020 provides two guarantees, namely: the decision of NAARC must be motivated and the measure must be brought to the attention of users. Also, the clarifications brought by the Ministry of Internal Affairs by specifying, on the 16th of March 2020, that 'This instrument (Article 54 of Decree no. 195/2020) concerns the fight against any misinformation action whose purpose is to induce panic through publications without identity or publications that systematically present information without real basis. The analysis will be carried out on a case-by-case basis and a prior dialogue with the representatives of the publication (if they can be identified) will be open, which could be the subject of such an analysis'.

However, the concrete analysis of information as 'fake news' can be an extremely difficult step. A large study carried out at the request of the Council of Europe has shown how complex these situations - in which incorrect information can be obtained - can be. Sometimes it can be about the gross falsification of some data or their manipulation or practices totally devoid of journalistic professionalism such as 'clickbait headlines' which were sadly frequently used during this period of lockdown.

One can observe the fact that not all news are founded on real information, and that everyone should inform themselves about the effects of a state of

emergency. and in which cases some fundamental rights can and should be restricted.

If one were to grade the level of freedom of expression in our country, on a rank from one to five, it would receive a five, but everyone should be aware of the fact that spreading fake news can lead to negative consequences and could misinform others massively. However, everyone should try to read as much as possible about a situation that they do not master and respect the obligations implemented by the government. It is fundamental in a democratic society that its population should be able to express themselves freely, but even fundamental rights, such as freedom of expression should be censored in some specific situations.

11. How do you overall assess the legal situation in your country regarding internet censorship?

Romanian legislation and regulations on internet censorship have continuously developed, and partially succeeded in adapting properly to the dynamic evolution that characterises the Virtual Era. In accordance to this, there are certain legal domains that are worthy of mention from the point of view of their progression in the matter of freedom of expression online: personal data protection (GDPR), cyber-bullying and hate speech, child pornography, discrimination on various grounds, e-commerce and illegal acts provided in the Penal Code.

An overall assessment would conclude in an optimistic final report. Consequently, it would state that Romania has implemented comprehensive and adequate measures that ensure the protection of fundamental, constitutional rights, including human dignity and the right to private life. The fight against unlawful and illegal internet content has determined the apparition and reinforcement of authorities, which now can be considered gatekeepers of fundamental rights and liberties of the individuals.

Thus, being intermediaries between the people and the State, the aforementioned authorities have taken on the role of both arbitrator and educator of a society in need of guidance.

The report tackles, amongst other things, issues of high importance to current society. Therefore, certain passages are dedicated to the *mise en œuvre* of national and transnational legislation during the state of emergency established due to the current pandemic crisis. The president of the National Council for Combating Discrimination (NCCD) described the online environment as subjected to a big

enhancement of hate speech. In addition, national authorities are facing a real issue regarding the spread of false information through online platforms. In spite of constant reassurance that the situation of hate speech and delivery of false information will ameliorate, we remain skeptic.

Looking ahead to the future, it is considered that the legislator should adopt measures that lead to a more accentuated balance between fundamental rights and liberties and to a prompter response to the rapid increase of illegal actions committed online. Nevertheless, establishing said balance poses certain risks that must be taken into account. For instance, censorship, whether it is directly enforced or measures are being implemented in order to obtain dissimulated restrictions, is often described as incompatible with a modern democratic society. This opinion is valid as long as one admits an undeniable necessity of censoring online content exists, in exceptional cases.

In light of the obvious truth that the legislator is not an omnipotent body, the growth in protection and prevention of unlawful and illegal activity with regard to the freedom of expression online will also reside in the hands of doctrinaires and practitioners, through specialised papers and statements, jurisprudence and guidelines.

Conclusion

As we have tried to prove, the issue of internet censorship is extremely vast and difficult to present within one single report. As a result, we are aware of the fact that we have not exhausted the subject, yet we believe to have emphasised, at least, the great variety of cases in which censorship may be encountered.

While comprehending that censorship may be used by authorities in a lot of various, different situations, we believe that it still remains the last resort to which authorities should refer to. This does not mean that it is intrinsically bad, yet it is potentially dangerous for the freedom of people – both individual and collective freedom. This is somehow paradoxical, given the fact that there are cases (exceptional cases, that is true) in which censorship itself is used for the preservation of a certain right – the right to be informed. This right to be informed implies the need for valuable, science-based, unbiased piece of information.

The decision of authorities to impose some form of censorship must be taken only after a thorough analysis of the issue, from which it is to be very clear that censorship is the only way to resolve a certain problem.

We are always to understand each and every individual right in relation to other human rights. We have to permanently keep in mind the ideal of a balance – in our case, the balance between the freedom of expression and the right to be informed, the balance between individual freedom of expression and national security. Balance is key, given that it is not *absolute rights* we should refer to, but rather *relative prerogatives* humans have, that sometimes may have to be adapted to given circumstances. Still, such an adaptive process is to remain of an exceptional nature, because only the exercise of a right is to be modified, not the essence of the right itself, which shall never be altered.

Table of legislation

Provision in Romanian language	**Corresponding translation in English**
Constituţia României	Constitution of Romania
Articolul 11 – Dreptul international şi dreptul intern (2) Tratatele ratificate de Parlament, potrivit legii, fac parte din dreptul intern.	Article 11 – International law and national law (2) International treaties ratified by the Parliament, according to the legal provisions, are part of the internal law.
Articolul 30 — Libertatea de exprimare (1) Libertatea de exprimare a gândurilor, a opiniilor sau a credințelor şi libertatea creațiilor de orice fel, prin viu grai, prin scris, prin imagini, prin sunete sau prin alte mijloace de comunicare în public, sunt inviolabile. (2) Cenzura de orice fel este interzisă. (3) Libertatea presei implică şi libertatea de a înființa publicații. (4) Nici o publicație nu poate fi suprimată. (…) (6) Libertatea de exprimare nu poate prejudicia demnitatea, onoarea, viața particulară a persoanei şi nici dreptul la propria imagine. (7) Sunt interzise de lege defăimarea ţării şi a naţiunii, îndemnul la război de agresiune, la ură naţională, rasială, de clasă sau religioasă, incitarea la discriminare, la separatism teritorial sau la violenţă publică, precum şi manifestările obscene, contrare bunelor moravuri. (…)	Article 30 — Freedom of expression (1) Freedom of expression of thoughts, opinions, or beliefs, and freedom of any creation, by words, in writing, in pictures, by sounds or other means of communication in public are inviolable. (2) Any censorship shall be prohibited. (3) Freedom of the press also involves the free setting up of publications. (4) No publication shall be suppressed. (…) (6) Freedom of expression shall not be prejudicial to the dignity, honour, privacy of a person, and to the right to one's own image (7) Defamation of the country and of the nation, instigation to war of aggression, any national, racial, class or religious hatred, incitement to discrimination, to territorial separatism or public violence, as well as obscene manifestations are prohibited by law.
Articolul 31 — Dreptul la informaţie (1) Dreptul persoanei de a avea acces la orice informaţie de interes public nu poate fi îngrădit. (2) Autorităţile publice, potrivit competenţelor ce le revin, sunt obligate să asigure informarea corectă a cetăţenilor asupra treburilor publice şi asupra problemelor de interes personal. (3) Dreptul la informaţie nu trebuie să prejudicieze măsurile de protecţie a tinerilor sau securitatea naţională.	Article 31 — Right to information (1) A person's right of access to any information of public interest shall not be restricted. (2) The public authorities, according to their competence, shall be bound to provide correct information to the citizens in public affairs and matters of personal interest. (3) The right to information shall not be prejudicial to the measures of protection of young people or national security. (4) Public and private media shall be bound to provide correct information to the public opinion.

(4) Mijloacele de informare în masă, publice şi private, sunt obligate să asigure informarea corectă a opiniei publice. (5) Serviciile publice de radio şi de televiziune sunt autonome. Ele trebuie să garanteze grupurilor sociale şi politice importante exercitarea dreptului la antenă. Organizarea acestor servicii şi controlul parlamentar asupra activităţii lor se reglementează prin lege organică.	(5) Public radio and television services shall be autonomous. They must guarantee any important social and political group the exercise of the right to broadcasting time. The organization of these services and the parliamentary control over their activity shall be regulated by an organic law.
Articolul 53 — Restrângerea exerciţiului unor drepturi sau al unor libertăţi (1) Exerciţiul unor drepturi sau al unor libertăţi poate fi restrâns numai prin lege şi numai dacă se impune, după caz, pentru: apărarea securităţii naţionale, a ordinii, a sănătăţii ori a moralei publice, a drepturilor şi a libertăţilor cetăţenilor; desfăşurarea instrucţiei penale; prevenirea consecinţelor unei calamităţi naturale, ale unui dezastru ori ale unui sinistru deosebit de grav. (2) Restrângerea poate fi dispusă numai dacă este necesară într-o societate democratică. Măsura trebuie să fie proporţională cu situaţia care a determinat-o, să fie aplicată în mod nediscriminatoriu şi fără a aduce atingere existenţei dreptului sau a libertăţii.	Article 53 — Restriction on the exercise of certain rights or freedoms (1) The exercise of certain rights or freedoms may only be restricted by law, and only if necessary, as the case may be, for: the defence of national security, of public order, health, or morals, of the citizens' rights and freedoms; conducting a criminal investigation; preventing the consequences of a natural calamity, disaster, or an extremely severe catastrophe. (2) Such restriction shall only be ordered if necessary in a democratic society. The measure shall be proportional to the situation having caused it, applied without discrimination, and without infringing on the existence of such right or freedom.
Legea audiovizualului nr. 504/2002, Articolul 6: (1) Cenzura de orice fel asupra comunicării audiovizuale este interzisă. (2) Independenţa editorială a furnizorilor de servicii media audiovizuale este recunoscută şi garantată de prezenta lege. (…)	Audiovisual law no. 504/2002, Article 6: (1) Censorship of any kind upon audio-visual communication is forbidden. (2) Editorial independence of audiovisual media services providers is acknowledged and warranted by this Law. (…)
Noul Cod Civil	New Civil Code
Articolul 253 (1) Persoana fizică ale cărei drepturi nepatrimoniale au fost încălcate ori ameninţate poate cere oricând instanţei: a) interzicerea săvârşirii faptei ilicite, dacă aceasta este iminentă; b) încetarea încălcării şi interzicerea pentru viitor, dacă aceasta durează încă; c) constatarea caracterului ilicit al faptei săvârşite, dacă tulburarea pe care a produs-o subzistă. (2) Prin excepţie de la prevederile alin. (1), în cazul încălcării drepturilor nepatrimoniale prin exercitarea dreptului la libera exprimare,	Article 253 (1) The natural person whose non-patrimonial rights have been violated or threatened may at any time request the court: a) the prohibition of committing the unlawful act, if it is imminent; b) the cessation of the infringement and the prohibition for the future, if it still lasts; c) ascertaining the unlawful nature of the act committed, if the disorder that it produced subsists. (2) By exception from the provisions of par. (1), in case of violation of non-patrimonial rights by exercising the right to free

instanţa poate dispune numai măsurile prevăzute la alin. (1) lit. b) şi c). (3) Totodată, cel care a suferit o încălcare a unor asemenea drepturi poate cere instanţei să îl oblige pe autorul faptei să îndeplinească orice măsuri socotite necesare de către instanţă spre a ajunge la restabilirea dreptului atins, cum sunt: a) obligarea autorului, pe cheltuiala sa, la publicarea hotărârii de condamnare; b) orice alte măsuri necesare pentru încetarea faptei ilicite sau pentru repararea prejudiciului cauzat.	expression, the court can order only the measures provided in par. (1) letter. b) and c). (3) At the same time, the person who has suffered an infringement of such rights may ask the court to compel the perpetrator to take any measures deemed necessary by the court to reach the restoration of the right attained, such as: a) order the author, at his expense, to publish the conviction decision; b) any other measures necessary to end the wrongful act or to repair the damage caused.
Articolul 70 - Dreptul la libera exprimare (1) Orice persoană are dreptul la libera exprimare. (2) Exercitarea acestui drept nu poate fi restrânsă decât în cazurile şi în limitele prevăzute la articolul 75.	Article 70 - Freedom of expression (1) Any person has the right to freedom of expression. (2) Exercising this right can only be restricted in the cases and limits stated in article75.
Articolul 75 – Limitele (1) Nu constituie o încălcare a drepturilor prevăzute în această secţiune atingerile care sunt permise de lege sau de convenţiile şi pactele internaţionale privitoare la drepturile omului la care România este parte. (2) Exercitarea drepturilor şi libertăţilor constituţionale cu bună-credinţă şi cu respectarea pactelor şi convenţiilor internaţionale la care România este parte nu constituie o încălcare a drepturilor prevăzute în prezenta secţiune.	Article 75 - Limits (1) Infringements upon the rights stated in this section which are allowed by law or conventions and international pacts on human rights which Romania is a party to are not considered breaches. (2) Exercising constitutional rights and liberties in good faith and in accordance with the international pacts and conventions Romania is a party to is not a breach of the rights in this section.
Legea nr. 196 din 13 mai 2003 privind prevenirea si combaterea pornografiei: Articolul 7: (1) Persoanele care realizeaza site-uri cu caracter pornografic sunt obligate sa le paroleze, iar accesul la acestea va fi permis numai dupa ce s-a platit o taxa pe minut de utilizare, stabilita de realizatorul site-ului si declarata la organele fiscale. (2) Persoanele care realizeaza sau administreaza site-uri trebuie sa evidentieze clar numarul accesarilor site-ului respectiv, pentru a putea fi supus obligatiilor fiscale prevazute de lege. (3) Se interzic realizarea si administrarea site-urilor avand caracter pedofil, zoofil sau necrofil.	Law no. 196 of 13 May 2003 on the prevention and combating of pornography: Article 7: (1) Persons who create pornographic sites are obliged to password them, and access to them will only be allowed after a fee per minute of use, established by the site's creator and declared to the tax authorities, has been paid. (2) Persons who create or manage sites must clearly highlight the number of accesses to the respective site, in order to be subject to the tax obligations provided by law. (3) The creation and administration of sites having a pedophile, zoophile or necrophiliac character is prohibited. Article 14:

Articolul 14: (1) Autoritatea Nationala de Reglementare in Comunicatii si Tehnologia Informatiei primeste sesizari cu privire la nerespectarea prevederilor Article 7. (2) in cazul primirii unei sesizari si al verificarii continutului site-ului, Autoritatea Nationala de Reglementare in Comunicatii si Tehnologia Informatiei solicita furnizorilor de servicii pentru internet blocarea accesului la site-ul in cauza. (3) Nerespectarea de catre furnizorii de servicii pentru internet a obligatiei de a bloca accesul la site-urile care nu respecta prevederile Article 7, in termen de 48 de ore de la primirea solicitarii prevazute la alin. (2) din partea Autoritatii Nationale de Reglementare in Comunicatii si Tehnologia Informatiei, constituie contraventie si se sanctioneaza cu amenda de la 10.000 lei la 50.000 lei.	(1) The National Regulatory Authority for Communications and Information Technology receives notifications regarding the non-observance of the provisions of Article 7. (2) in case of receiving a notification and verifying the content of the site, the National Regulatory Authority in Communications and Information Technology requests the Internet service providers to block access to the site in question. (3) Non-compliance by the Internet service providers of the obligation to block access to sites that do not comply with the provisions of Article 7, within 48 hours after receiving the request provided in par. (2) from the National Regulatory Authority for Communications and Information Technology, constitutes a contravention and is sanctioned with a fine from 10,000 LEI to 50,000 LEI.
Decretul 195/2020 Articolul 54: (3) Furnizorii de servicii de găzduire si furnizorii de continut sunt obligati ca, la decizia motivată a Autorităţii Nationale pentru Administrare si Reglementare în Comunicatii, să întrerupă imediat, cu informarea utilizatorilor, transmiterea într-o retea de comunicatii electronice ori stocarea continutului, prin eliminarea acestuia la sursă, dacă prin continutul respectiv se promovează stiri false cu privire la evolutia COVID-19 si la măsurile de protectie si prevenire.	Decree 195/2020 Article 54: (3) The hosting service providers and the content providers are obliged, at the motivated decision of the National Authority for Administration and Regulation in Communications, to immediately interrupt, with informing the users, the transmission in an electronic communications network or the storage of the content, by its elimination at source, if the content promotes false news about the evolution of COVID-19 and protection and prevention measures.
Anexa 1 la Decretul 240/2020 Articolul 91: (3) Furnizorii de servicii de găzduire şi furnizorii de conţinut sunt obligaţi ca, la decizia motivată a Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii, să întrerupă imediat, cu informarea utilizatorilor, transmiterea într-o reţea de comunicaţii electronice ori stocarea conţinutului, prin eliminarea acestuia la sursă, dacă prin conţinutul respectiv se promovează ştiri	Annex no. 1 to Decree 240/2020 Article 91: (3) Hosting providers and content providers are obliged to, at the reasoned decision of The National Authority for Administration and Regulation in Communications, to interrupt immediately, with user information, transmission in an electronic communications network or storage content, by removing it from the source, if the content promotes news false information on the evolution of COVID-19 and on protection and prevention measures.

false cu privire la evoluţia COVID-19 şi la măsurile de protecţie şi prevenire.	
Codul Penal din 1969 (abrogat) – Articolul 205: "Atingerea adusă onoarei ori reputaţiei unei persoane prin cuvinte, prin gesturi sau prin orice alte mijloace, ori prin expunerea la batjocură, se pedepseşte cu închisoare de la o lună la 2 ani sau cu amendă."	Penal Code from 1969 (abrogated) - Article 205: "Interference to honour or reputation of a person through words, gestures or any other means, or exposure to mockery is punished with imprisonment from one month to 2 years or with fine."
Articolul 206 Cod Penal 1969 (abrogat): "Afirmarea ori imputarea în public, prin orice mijloace, a unei fapte determinate privitoare la o persoană, care, dacă ar fi adevărată, ar expune acea persoană la o sancţiune penală, administrativă sau disciplinară ori dispreţului public, se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă."	Article 205 Penal Code from 1969 (abrogated): "Affirming or imputing in public, by any means, a determined deed regarding a certain person, which, if it were true, it would expose that person to a penal, administrative or disciplinary sanction or public contempt, is punished with imprisonment from 3 months to 3 years ori with fine."

Bibliography

English titles

Legislation

The European Convention of Human Rights

Regulation (EU) 2016/679 of The European Parliament and of The Council

Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech" (Adopted by the Committee of Ministers on 30 October 1997 at the 607th meeting of the Ministers' Deputies)

Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech" (adopted by the Committee of Ministers on 30 October 1997 at the 607th meeting of the Ministers' Deputies)

Reports

Information Disorder - Toward an interdisciplinary framework for research and policymaking, Claire Wardle, PhD and Hossein Derakhshan, Council of Europe, October 2017, page 73

Books

Freedom of Expression and The Internet, Wolfgang Benedek and Matthias C. Kettemann, Council of Europe Publishing, 2013, page 83-85

Periodicals

Hate-Speech in the Romanian Online Media, Radu M. Meza, Journal of Media Research, vol.9 issue 3(26)/2016, <https://www.academia.edu/30173854/Hate_speech_in_the_Romanian_Online_Media>, accessed 18 May 2020

Digital resources

Daphne Keller, The Center for Internet and Society, 'Notice and Takedown Under the GDPR: An Operational Review' <http://cyberlaw.stanford.edu/blog/2015/10/notice-and-takedown-under-gdpr-operational-overview?fbclid=IwAR2mvzQPDupIpBfcOUrC0pRWmbVsJNy5vaeV0y9SJc4a5uEY37MPAVf1tB0>, accessed 18 May 2020

Information Commissioner's Office, 'GDPR Principles' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>, accessed 18 May 2020

NIBUSINESSINFO, 'Data protection principles under the GDPR' <https://www.nibusinessinfo.co.uk/content/data-protection-principles-under-gdpr>, accessed 18 May 2020

Information Commissioner's Office, 'What is personal data?' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/>, accessed 18 May 2020

Romanian titles

Legislation

The Constitution of Romania

The Romanian Civil Code from 2011

The Romanian Penal Code from 1969

The Romanian Penal Code from 2014

Law no. 196 of 13 May 2003 on the prevention and combating of pornography in Romania

Audiovisual Law no. 504/2002

O.G. 137/2000 regarding prevention and sanction of all forms of discrimination

O.U.G. 31/2002 regarding the prohibition of organisations, simbols and acts with fascist, legionary, rasist or xenophobic character and promoting the cult of personalities condemned of committing felonies of genocide, crimes against humanity and war crimes

Decision no. 220/2011 regarding the Regulatory Code of audiovisual content

Reports

Freedom of speech in the Romanian legislation, Diana Olivia Hatneanu, Centrul pentru Jurnalism Independent, 2013, < http://cji.ro/wp-content/uploads/2020/04/13.-Libertatea-de-exprimare-in-legislatia-romaneasca-Final-2.pdf >, accessed 18 May 2020

A comparative analysis over the legislation and case law in the field of discriminatory or hate speech, Iustina Ionescu, Adriana Iordache, research realised with the support of Open Society Foundations (OSF), Think Tank Fund and Roma Initiatives Office, September 2015, available here

Books

Administrative Law, Vol II, Dana Apostol Tofan, 4th edition, Ed. C. H. Beck, 2017, ISBN 978-606-18-0734-5, page 41

Periodicals

Introduction to Civil Law, Ionel Reghini, Serban Diaconescu, Paul Vasilescu, Ed. Hamangiu, 2013, page 360

Explanatory Dictionary of the romanian language (2nd edition, revised and completed), Romanian Academy, Linguistics Institute, 2009

Digital resources

ActiveWatch, 'Annual Report on Intolerant Discourse and Hate Speech, 2018' <https://activewatch.ro/Assets/Upload/files/Raport_ActiveWatch_Hate_Speech_2018.pdf>, accessed on 29 April 2020

ActiveWatch, 'Annual Report on Intolerant Discourse and Hate Speech, 2018' <https://activewatch.ro/Assets/Upload/files/00_Raport%20hate%20speech_final%20(1).pdf>, accessed on 29 April 2020

Digi24, Alexandru Costea, 'Explosion of hate in the public sphere' <https://www.digi24.ro/stiri/actualitate/politica/a-explodat-ura-in-spatiul-public-cncd-analizeaza-un-val-de-plangeri-pentru-rasism-atacuri-la-bor-si-discriminarea-catolicilor-1293558>, accessed on 2 May 2020

CNCD, <https://cncd.ro/discriminare>, accessed on 25 April 2020

UNBR, 'Protecting freedom of speech in the context of national efforts to combat illegal and harmful content on the internet' < http://www.unbr.ro/protectia-libertatii-de-exprimare-in-contextul-eforturilor-statelor-de-combate-a-continului-ilegal-si-daunator-pe-internet-comunicare-sustinuta-de-doamna-avocat-monica-cercelescu-in-cadrul-seminarul/>, accessed 3 February 2020

JURIDICE, Cristina Staicu, 'Cyberbullying – Legal challenges. Do you know you're your child is up to?' < https://www.juridice.ro/550662/cyberbullyingul-provocari-legislative-tu-stii-ce-mai-face-copilul-tau.html>

Wikipedia, 'Communism and Romanian Press' <https://ro.wikipedia.org/wiki/Comunismul_şi_presa_românească>, accessed 18 May 2020

PEROL.RO, 'Two other sites closed down by ANCOM for spreading fake news in the midst of the coronavirus pandemic' <https://perol.ro/alte-doua-site-uri-inchise-de-ancom-pentru-raspandirea-de-stiri-false-in-plina-pandemie-de-coronavirus/?fbclid=IwAR1pZTV0R49_zkI-fvB8rssAO_YpuEa7oH_eQZXeHhh2ePDjXrKXOG8ptBI>, accessed 18 May 2020

CAPITAL, Alexandra Buican, 'The main sources of information for Romanian people' <https://www.capital.ro/principalele-surse-de-informare-pentru-romani-studiu.html>, accessed 31 May 2020

Case law

Decision no. 62/2007 of the Constitutional Court of Romania

ELSA Serbia

Contributors

National Coordinator

Anđela Mirić

National Researchers

Dina Ivetić

Sofija Stojanović

Nevena Glušac

Luka Todorić

Nikola Todorović

Jovana Anja Građanski

Olivera Nećak

National Linguistic Editor

Miloš Mirović

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

Freedom of Expression is protected by various laws in the Republic of Serbia: the Constitution of Republic of Serbia[1795], the Act on public Information and media[1796], the Act on free access to information of public importance[1797], the Act on electronic media[1798] and the Criminal Code[1799]. Article 46 of **The Constitution of Republic of Serbia** proclaims the freedom of thought and expression and states that it may be restricted by the law if necessary to protect rights and reputation of others, to uphold the authority and objectivity of the court and to protect public health, morals of a democratic society and national security of the Republic of Serbia. Several other articles are also important like Article 50 (Freedom of Media)[1800] and Article 51 (Right to Information)[1801], some that regulate this matter indirectly, like prohibition of discrimination[1802] , and several articles on rights of the minorities that proclaim freedom of expression among their other rights. **Act on public information and media** also prohibits censorship and states that 'free flow of information through media must not be endangered, nor editor media autonomy, especially by applying force, threat, or by blackmail towards an editor, reporter or a source of information'[1803]. This act protects the pluralism of media[1804], which ensures the Right to Information and states that the court can, if the public prosecutor files a motion, forbid distributing of the information or other media content, if necessary in the democratic society and if the information calls for: 1) an act of direct and violent tear-down of the constitutional order; 2) an act of direct violence towards a person or a group base on the race, ethnicity, political affiliation, religion, sexual

1795 «Official Gazette of the RS» no. 98/2006.

1796 «Official Gazette of the RS» no. 83/2014, 58/2015 and 12/2016 – authentic interpretation.

1797 «Official Gazette of the RS» no. 120/2004, 54/2007, 104/2009 and 36/2010.

1798 «Official Gazette of the RS» no. 83/2014 and 6/2016.

1799 «Official Gazette of the RS» no. 85/2005, 88/2005 – correction, 107/2005 - correction, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.

1800 Paragraph 3: 'Censorship shall not be applied in the Republic of Serbia. Competent court may prevent the dissemination of information through means of public informing only when this is necessary in a democratic society to prevent inciting to violent overthrow of the system established by the Constitution or to prevent violation of territorial integrity of the Republic of Serbia, to prevent propagation of war or instigation to direct violence, or to prevent advocacy of racial, ethnic or religious hatred enticing discrimination, hostility or violence.'

1801 'Everyone shall have the right to be informed accurately, fully and timely about issues of public importance. The media shall have the obligation to respect this right. Everyone shall have the right to access information kept by state bodies and organizations with delegated public powers, in accordance with the law.'

1802 Article 21.

1803 Article 4.

1804 Article 45-47.

orientation, disability or other personal characteristics, if publishing the information directly threats to inflict serious and irreparable consequences that cannot be prevented any other way[1805]. The presumption of innocence, the prohibition of hate speech[1806], protection of minors and prohibition of public display of pornography are also cited in this Act. **The Act on free access to information of public importance** establishes an institution of the Commissioner for information of public importance and personal data protection. This Commissioner can command government bodies to provide the right to information to a person that was withheld from it. The Act sets limitations to the free access to information of public importance if life, health, security, judiciary, defence of the country, national and public security, the economic well-being of the country and secrecy is endangered by providing that information to the applicant[1807]. Also, the Right to Information shall be denied if the Right to Privacy, Right to Reputation or any other right would be infringed[1808]. **The Act on electronic media** establishes the Regulatory authority for electronic media which goal is to, amongst others, contribute to the preservation, protection and development of the freedom of thought and expression[1809]. This act also proclaims duty to respect human rights, prohibits hate speech, protects the rights of the disabled and copyright and related rights. The protection of minors is also established[1810] through the prohibition of displaying pornography, scenes of brutal violence and other content that can severely harm the physical, mental or moral development of a minor. As for the criminal aspects of the freedom of expression, **Criminal Code** incriminates insult[1811], but it no longer considers defamation a criminal activity. It also contains criminal offences against intellectual property and some of them are 'Unauthorised Use of Copyrighted Work or other Work Protected by Similar Right'[1812] and 'Unauthorised Removal or Altering of Electronic Information on Copyright and Similar Rights'[1813], which represents a limitation to the Right to Information. The Criminal Code incriminates 'Violation of Confidentiality of Proceeding'[1814]. The Republic of Serbia is also a member state of the **European Convention on Human Rights** (since 2004) **and of the UN International**

1805 Article 59.
1806 Article 75.
1807 Article 9.
1808 Article 14.
1809 Article 5.
1810 Article 68.
1811 Article 170.
1812 Article 199.
1813 Article 200.
1814 Article 337.

Covenant on Civil and Political Rights (since 1992), which proclaim freedom of thought and expression.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

Censorship is defined as the overview of content prepared for printing, radio and TV-shows, movies, plays, etc. done by political or religious authorities or even by private persons before or after the emission, with the purpose of restricting or prohibiting publishing of the content contrary to the interests of the public morals, the interest of the church or political organisations. In democratic societies censorship is an exceptional measure. [1815]

The Constitution of the Republic of Serbia grants freedom of thought and expression as well as freedom of media. Also, in Article 50 Paragraph 3 The Constitution prohibits censorship:

'Censorship shall not be applied in the Republic of Serbia'[1816]

The same Article limits the freedom of media in accordance with Article 10 Paragraph 2 of the European Convention on Human Rights which allows the High Contracting Parties to limit freedoms and rights granted by the Convention[1817] if the certain criteria given by the European Court of Human Rights jurisprudence is fulfilled. In the case Handyside v United Kingdom the Court established criteria to determine whether the limitation of the right or freedom is just or not. [1818] Necessary requirements in order of validation of the restriction are following:

1) the limitation has to be foreseen by the law,

2) the limitation has to be justified by a legitimate purpose (in agreement to Article10 Paragraph 2),

3) the limitation has to be necessary in a democratic society,

4) the limitation has to be proportional to the legitimate purpose pursued. [1819]

Article 50 Paragraph 2 reads as follows:

[1815] Pravna enciklopedija (1st edn, 1979), page 146.
[1816] Constitution of Republic of Serbia (Official Gazette of Republic of Serbia no. 98/2006).
[1817] Steven Greer, The exceptions to Articles 8-11 of the European Convention on Human Rights (Council of Europe Publishing, 1997), page 6.
[1818] *Handyside v. United Kingdom* App. no. 5493/72, (ECHR 7th December 1976), page 49.
[1819] Final Report International Legal Research Group On Freedom of Expression And Protection Of Journalistic Sources (ELSA, 2016), page 1439.

'Competent court may prevent the dissemination of information through means of public informing only when this is necessary in

a democratic society to prevent inciting to violent overthrow of the system established by the Constitution or to prevent violation of territorial integrity of the Republic of Serbia, to prevent propagation of war or instigation to direct violence, or to prevent advocacy of racial, ethnic or religious hatred enticing discrimination, hostility or violence'.

Theory and practice are familiar with three means of censorship: preliminary (preventive) censorship, retroactive (suspensive) censorship and self-censorship.[1820] In the Republic of Serbia, there is no preliminary censorship. When it comes to retroactive censorship, there are only three legislative acts that prescribe taking down of internet content: Law of Electronic Commerce Advertising Law and Law on Personal Data Protection; while blocking of the content is not regulated by the State. Authorities in Serbia rely on self-censorship of the authors and publishers of internet content and prescribe which content will be considered inadequate to be published, as it can be seen in following acts: Law on Radio-Diffusion, Law on Public Information and Media, Law on Electronic Media and Criminal Code. For the violations of the provisions of these legal acts, the legislative body of Republic of Serbia prescribes sanctions that vary from warning to revoking the licence for publishing.

Law of Electronic Commerce[1821] prescribes the obligation of the service provider to take down the inadequate content at the request of the competent state authority or the third party in Article 20 Paragraph 5, 6 and 7:

'The provider of the information society is obliged to remove the prohibited content without delay no later than two working days after the day of receiving of the act of the competent state authority, ordering removal of the illegal content. The competent authority shall issue an act ex officio or at the request of a party.

At the request of a third party, the service provider of the information society is obliged to remove the prohibited content without delay within two working days of receiving the request of that person at the latest, unless it considers that the published content does not contravene the provisions of the law. In this case, the service provider may contact the competent state authority and request that

[1820] Irma Ratiani, Totalitarianism and Literary Discourse: 20th Century Experience (Cambridge Scholars Publishing, 2012), page 359 Philip Cook, Conrad Heilmann, Censorship and Two Types of Self Censorship, LSE Choice Group working paper series, vol. 6, no. 2 (The Centre for Philosophy of Natural and Social Science (CPNSS), London School of Economics, 2010), page 14.

[1821] Law on Electronic Commerce (Official Gazette of Republic of Serbia no. 41/2009, 95/2013, 52/2019).

the competent authority determine whether the provisions of the law have been violated in the specific case, which necessitates the removal of the content.

The act of the competent authority from Paragraphs 5 and 6 of this Article, which requires the service provider to remove inappropriate content, must contain a precise description of the site on the website, or other electronic display on which the inappropriate content appears, as well as the explanation of the inadmissibility'. Other legal act that prescribes taking down the content is Law on Personal Data Protection[1822] in Article 30 Paragraph 2:

'If the person in charge of handling the data made personal data public, his obligation to delete data shall also include taking all reasonable measures, including technical measures, in accordance with the available technologies and capabilities to bear the costs of their use, in order to inform other data operators that the person on whom the data subject has submitted a request for taking down all the copies and electronic links to this data.'

Advertising Law[1823] devotes following Articles to the matter of content of internet advertising:

Article 7:

'The advertising, which recommends the advertiser, the activity or the production and marketing of goods and services which are prohibited by law or by an individual act of the competent authority is prohibited.

If the subject of advertising is an activity that can be performed only on the basis of consent, permit or other act of a state authority, advertising shall be prohibited unless the consent, permit or other act of the competent authority is issued. It is forbidden to advertise that calls for illicit actions towards others or boycotting of others, or ending or preventing relations with them.'

Article 8:

'It is forbidden that the advertising message, directly or indirectly, encourages discrimination on any grounds, especially on the grounds of belief, national, ethnic, religious, gender or racial origin, political, sexual or other orientation, social origin, property status, culture, language, age, or mental or physical disability.'

According to Articles 47-57 and Articles 59-61 it is forbidden to advertise alcoholic beverages, tobacco industry products, games of luck, lottery, prize games, narcotics and controlled psychoactive substances, pornography, weapon

[1822] Law on Personal Data Protection (Official Gazette of Republic of Serbia no. 87/2018).
[1823] Advertising Law (Official Gazette of Republic of Serbia no. 6/2016, 52/2019).

and military equipment contrary to the provision of this law. Article 58 prescribes that advertisements containing health or nutrition-related statements must be based on scientific and professional research.

Article 45 Paragraph 7 prescribes taking down of the inadmissible content:

'If, during the inspection procedure, the competent authority determines that the content of the advertisement message is contrary to the provisions of this law, it shall issue a decision to the transferor of the advertisement message to take down such a message and leave it a reasonable deadline, which may not be shorter than three nor longer than eight days from the date of receiving of the decision.'

One of the main principles of the Law on Radio-Diffusion[1824] is the prohibition of discrimination expressed in Article 3 of this law. Article 19 prohibits programs that severely endanger the physical, mental or moral development of the minors and Article 21 prohibits diffusion of information that encourage discrimination, hatred or violence against a person or group of people because of a different political orientation or belonging or not belonging to a race, religion, nation, ethnic group or discrimination, hatred or violence based on gender or sexual orientation. Article 68 prohibits broadcasting programs that contain pornography or whose content highlights and supports violence, drug addiction or other criminal behaviour, as well as abusive programs. By this Article it is also forbidden to advertise political organisations outside the election campaign. Republic Radio-Diffusion Agency established by this law has no censor the content, but it allowed by Article 17 of this law to revoke the licence for the radio-diffusion, temporary or permanently, for the violation of the previously listed Articles.

Law on Public Information and Media[1825] forbids hate speech in Article 75. This law prescribes prohibition of distribution of inadmissible information and content in following Articles:

Article 59:

'At the proposal of the competent public prosecutor, the competent court may prohibit the distribution of information or other media content (in further text: information) if that is necessary in a democratic society and if the information refers to:

[1824] Law on Radio-Diffusion (Official Gazette of Republic of Serbia no. 42/2002, 97/2004, 76/2005, 79/2005, 62/2006, 85/2006, 86/2006).

[1825] Law on Public Information And Media (Official Gazette of Republic of Serbia no. 83/2014, 58/2015, 12/2016).

1) an act of direct violent overthrow of the constitutional order;

2) an act of direct violence against a person or group on the basis of race, nationality, political affiliation, religion, sexual orientation, disability or other personal property, and if the publication of information directly threatens to cause serious and irreparable consequence that cannot be prevented otherwise.'

Article 60:

'The proposal for the prohibition of distribution of information (in further text: the prohibition proposal) is submitted by the competent public prosecutor. The Prohibition Proposal may require the prohibition of the distribution of the information referred to in Article 59 of this Law, the seizure of newspapers containing such information if the purpose of the prohibition can only be achieved in that way, or the prohibition of the dissemination of such information through other media.'

Aside from the public prosecutor, person whose rights or interests are violated by the published content or information may protect them in accordance with Article 101 which reads as follows:

'If the publication of information or records violates the presumption of innocence, the prohibition of hate speech, the rights and interests of minors, the prohibition of public exposure of pornographic content, the right to dignity of the person, the right to authenticity, or the right to privacy, in accordance with the provisions of this law, a lawsuit may require:

1) determination that the publication of information or records violates the right or interest;

2) non-publishing, as well as prohibiting the re-publication of information or records;

3) handing over of a record, removal or destruction of a published record (deletion of videos, deletion of audio records, destruction of negatives, removal from publications and the like). Law on Electronic Media[1826] in following Articles prescribes prohibitions and obligation that electronic media editors need to follow:

Article 47 forbids "providing programs that emphasise and support drug addiction, violence, criminal or other illicit behaviour, as well as content that abuses the gullibility of viewers and listeners.'

[1826] Law on Electronic Media (Official Gazette of Republic of Serbia no. 83/2014, 6/2016).

Article 50 prescribes obligation to 'respect the dignity of the person and human rights, and in particular take care not to show degrading treatment and scenes of violence and torture, unless there is programmatic and artistic justification.

Content that may impair the physical, mental or moral development of the minors must be clearly labelled and not published at a time when the minor may reasonably be expected to follow them, given the usual schedule of their activities, except exceptionally as a protected service with conditional access in a manner provided for by this law.'

Article 51 of this law prescribes that content can 'not contain information that encourages, in an open or covert manner, discrimination, hatred or violence due to race, colour, ancestry, citizenship, nationality, language, religious or political beliefs, gender, gender identity, sexual orientation, wealth, birth, genetic characteristics, health status, disability, marital and family status, conviction, age, appearance, membership in political organisations, trade unions and other organisations and other real or assumed personal characteristics.'

Article 68 protects the minors: Paragraph 1: 'It is prohibited to display pornography, scenes of brutal violence and other program content that can seriously harm the physical, mental or moral development of a minor.' Paragraph 10: 'Media service providers are required to clearly label programs that may endanger or are inappropriate for minors, as well as alert parents.'

This law establishes The Regulative Body for Electronic Media that is allowed to sanction the provider of media service for the violation of previously listed Articles in accordance with Article 28: 'The Regulative Body for Electronic Media may impose a warning, temporary prohibit the publication of content, or may revoke the license given to the provider of the media service due to violation of obligations related to program content, as well as due to violation of the conditions contained in the license or approval for the provision of media service in accordance with the provisions of this Law.'

Article 101 determines limitations considering protected services with conditional access:

'It is prohibited to create, import, market, lease, or hold for commercial purposes any funds, devices or software designed or adapted to enable access to the protected services in an intelligible form without the permission of the service provider or to facilitate circumvention of any measure of conditional access to the protected service. It is prohibited to install, maintain or replace the funds referred to in paragraph 1 of this Article for commercial purposes.

It is prohibited to circumvent any measure of conditional access or to provide or facilitate services.'

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

Legislation of the Republic of Serbia is consistent in a way that the grounds, under which removal or censorship of internet content is allowed, are narrowly limited to those providing protection of content which is important to the community and of public interest. Practice has shown that freedom of expression in Serbia is, in most cases, compromised due to the lack of transparency – particularly in the field of media ownership.[1827] One of the most prominent cases of non-transparent media ownership is the oldest Serbian daily newspaper 'Politika'. Although it was founded in 1904, to this day it has an unclear ownership structure given that its co-ownership share was bought by 'EastMedia Group' registered in Russia (which has dormant status in this country, due to inactivity) and the fact that 50% of the paper is still in state ownership, despite the law obliging the state to withdraw from media ownership.

Upon deciding whether limiting freedom of expression is legitimate in a particular case, the competent court conducts a three-step test in an emergency procedure, including providing answers to whether restrictive measures are in accordance with the law, whether they seek to achieve legitimate aim and if they are necessary in a democratic society. [1828]

Information and ideas which infringe rights and reputation of others, overturn the authority and objectivity of the court and endanger public health, morals of democratic and national security of the Republic of Serbia, may be restricted by law. [1829] This includes incitement of racial, ethnic and religious hatred, as prohibited and punishable under Article 49 of Constitution of The Republic of Serbia. Censorship over public information spread by the means of media, including internet, may only be applied by the competent courts if necessary to prevent accessory offences of inciting to violent overthrow of the system established by the Constitution and instigating to direct violence, violation of territorial integrity of the Country, propagation of war, as well as hateful speech which may lead to discrimination, violence and hostility. [1830]

[1827] Predrag Dimitrijević, Jelena Vučković, Analiza medijskog zakonodavstva u Republici Srbiji, Foundation Public Law Center, 2018, page 4.

[1828] ibid., page 5.

[1829] Article 46 in Constitution of the Republic of Serbia, National Authorities, 30 September 2006, Published in the Official Gazette of the Republic of Serbia, No 83/06.

[1830] Article 50. 46 in Constitution of the Republic of Serbia, National Authorities, 30 September 2006, Published in the Official Gazette of the Republic of Serbia, No 83/06.

Although Case law is not a source of law in the Republic of Serbia, it seems to point towards hateful and discriminatory speech as the primary grounds under which applications for removing the internet content are being made. An example would be a complaint from the Belgrade Centre for Human rights against the information portal 'Kurir', for allowing discriminatory and offensive comments to be available on the article that they shared on their Facebook profile (Article name: 'Disgrace! Morgan Freeman insulted Serbs: The actor accused us of committing Genocide!').

Primary law which regulates hate speech is Law on the Prohibition of Discrimination in which Article 11 prohibits the expression of ideas, information and opinions inciting discrimination, hatred or violence against person(s) because of their personal characteristics, in places accessible to the public, including mass media. The Law recognises three different remedies. First is a complaint filed by a person allegedly discriminated against to the Commissioner for the Protection of Equality. The Commissioner may only hand opinions on the violation of rights, along with recommendations of remedies to the injury, in cases of hate speech on the internet which occurred within the territory of the Republic of Serbia.[1831] This mechanism has potential to and should impact good practice of other competent authorities in combating hate speech. Another mechanism is litigation under which a plaintiff can file a claim for prohibition of discriminatory treatment or elimination of the consequences of discriminatory treatment, as well as compensation for pecuniary and non-pecuniary damage in the form of publication of the judgment. [1832]

Due to the length of litigation, the first mechanism would be preferable over the others if it weren't for the limited possibilities of conducting the proceedings against the persons whose identity cannot be determined, as well as the absence of retributive nature of the decision established this way. Final remedy is a misdemeanour charge in front of the Misdemeanour Court. The Law prescribes fines for violation of its certain provisions. [1833]

Law on Electronic Media enlists the Regulatory Body for Electronic Media as a responsible body in ensuring that the program content of the media service provider does not include one or more of the prohibited discriminatory grounds. These grounds are compiled in an exhaustive list and include race, colour, ancestry, citizenship, nationality, language, religious and political beliefs, gender and gender identity, sexual orientation, wealth, birth, genetic characteristics,

[1831] Articles 35-40 in Law on Prohibition of Discrimination, National Authorities, 26 March 2009, Published in the Official Gazette of the Republic of Serbia, No 22/09.
[1832] ibid., Articles 43-44.
[1833] ibid., Articles 50-60.

health status, disability, marital and family status, conviction, age, appearance, membership in political, trade union and other organisations and other real or assumed personal characteristics.[1834] Pornographic content, depictions of brutal violence and other program content which may seriously harm physical, mental or moral development of a minor is explicitly prohibited.[1835] The Law prescribes sanctioning fines in the event of either offence.[1836] Although the Regulatory Body for Electronic Media was intended to be an important independent regulator, its effectiveness leaves a lot to be desired due to the influence of legislative and executive power on financial independence and autonomy of decision-making, as well as the process of electing Council members and procedure of passing the REM statute. [1837]

Law on Advertising sets forth the inspection procedure and grounds under which the competent authority is obliged to order the removal of the advertisement messages posted on internet presentations, social media, applications or other means of internet communication. Firstly, these advertisements must be unequivocally directed to the recipients who are citizens of the Republic of Serbia and the object of the ads must be goods or services that can be purchased or delivered in the Republic of Serbia. Second, the transferor of the advertisement shall be ordered to remove the message in a timely manner in the event of said message failing to comply with the provisions of this Law.[1838] With that being said, provisions of this Law prohibit hateful, intolerant and discriminatory advertising, as well as advertising which incites endangering health and safety and advertising of goods, services or the advertisers prohibited by law.[1839] Article 71 of the Law on Advertising provides judicial protection for misleading advertising, which is forbidden and may by its deceptive nature affect the economic behaviour of the recipient or harm competitor advertisements. It also prohibits comparative advertising which identifies a competitor and/or its goods or services. [1840]

1834 Article 51 in Law on Electronic Media, National Authorities, 2 August 2014, Published in the Official Gazette of the Republic of Serbia, No. 83/2014 and No. 6/2016.
1835 ibid., Article 68.
1836 ibid., Articles 110 and 111.
1837 Predrag Dimitrijević, Jelena Vučković, Analiza medijskog zakonodavstva u Republici Srbiji, Foundation Public Law Center, 2018, page 14.
1838 Article 45 in Law on Advertising, National Authorities, 26 January 2016, Published in the Official Gazette of the Republic of Serbia, No. 6/2016 and No. 52/2019.
1839 ibid., Articles 6, 7, 8 and 10.
1840 ibid., Article 14.

Competent court may, in case of a lawsuit being filed, order the termination and/or correction of aforementioned advertising messages. [1841]

The Law on Public Information and Media also prohibits hate speech, in compliance with its definition as set forth in the Constitution, but exempts from liability if said information is a part of journalistic text and the intent behind publishing is providing objective journalistic report or criticism directed towards prohibited speech.[1842] It is important to note that this Law recognises internet forums, social media and other platforms, blogs, web and other electronic presentations as media, only if they are registered as such in The Media Register and in compliance with this Law.[1843] Competent courts may prohibit the distribution of information intended to violently overthrow the constitutional order or information which incites direct violence against a person or a group based on any of the aforementioned discriminatory grounds.[1844] Besides hate speech, this legislation prohibits publication of information which pertains to private life without the consent of the person it concerns and provides protection to the basic human right to privacy.[1845] On the other hand, consent may be deemed unnecessary if publication of such information is of public interest: for example, when it concerns a public office-holder and it is in the interest of national or public security, economic well-being of the country or prevention of crime. [1846]

Law on the Prohibition of the Manifestation of Neo-Nazi or Fascist Organizations and Associations prohibits presenting neo-Nazi and fascist propaganda materials or opinions which incite hatred and intolerance and jeopardise the legal order.[1847] This includes making such content available to the public by means of the internet.[1848] Up to this date, there hasn't been a single proceeding initiated on the grounds set forth in this legislation.

[1841] Article 71. in Law on Advertising, National Authorities, 26 January 2016, Published in the Official Gazette of the Republic of Serbia, No. 6/2016 and No. 52/2019.

[1842] Articles 75 and 76 in Law on Public Information and Media, National Authorities, 2 August 2014, Published in the Official Gazette of the Republic of Serbia, No. 83/2014, No. 58/2015 and No. 12/2016.

[1843] ibid., Article 29.

[1844] ibid., Article 59.

[1845] Article 80. Articles 75 and 76 in Law on Public Information and Media, National Authorities, 2 August 2014, Published in the Official Gazette of the Republic of Serbia, No. 83/2014, No. 58/2015 and No. 12/2016.

[1846] ibid., Article 82.

[1847] Article 3 in Law on the Prohibition of the Manifestation of Neo-Nazi or Fascist Organizations and Associations and Prohibition of use of Neo-Nazi or Fascist Symbols and Insignia, National Authorities, 29 May 2009, Published in the Official Gazette of the Republic of Serbia, No. 41/2009.

[1848] ibid., Article 6.

When it comes to the criminal procedure, The Criminal Procedure Code sets a legal framework and the Law on Organisation and Jurisdiction of Government Authorities for Suppression of Cybercrime governs establishing, organisation, jurisdiction and powers of special organisational units for detecting, prosecuting and trial for criminal offences stipulated in that Law. Article 4 of the aforementioned Law states that the prosecution of cybercrime is done by a special unit for suppression of cybercrime in the Higher Public Prosecutor in Belgrade, and that the Higher Court in Belgrade has the jurisdiction to trial the perpetrators of cybercrime. The procedure is regulated by The Criminal Procedure Code – the criminal charges shall be submitted to the special unit aforementioned which shall launch an investigation. After the investigation is done, the trial may begin if the public prosecutor gathered enough evidence for the prosecution. During the trial the evidence is presented to the judges and they shall decide whether or not to convict the supposed perpetrator.

In the case of Vjerica Radeta, the criminal charges were brought up against her for posting tweets that instigated or exacerbated national, racial or religious hatred or intolerance among the peoples and ethnic communities living in Serbia (paragraph 1, Article 317 of the Criminal Code) and that, on grounds of race, colour, religion, nationality, ethnic origin or other personal characteristic violated fundamental human rights and freedoms guaranteed by universally accepted rules of international law and international treaties ratified by Serbia, as well as propagated racial intolerance (paragraph 2 and 3, Article 387 of the Criminal Code). Further information about this case is unknown.

In Handyside v the UK, ECHR submits that not only information that is favourably received, but also the ideas which offend, shock or disturb the State are protected under Freedom of Speech.[1849] It is important to note, on the other hand, that democratic societies may sanction or prevent expression which incites intolerance-based hatred.[1850] There are various reasons as to why it is difficult to determine whether the legislation of the Republic of Serbia complies with the case law of ECHR. The number of initiated and processed lawsuits regarding hate speech is remotely low. In part, this possibly has something to do with a lack of proper definition which allows judicial bodies to act effectively upon initiation of proceedings, but as well with targeted persons or groups being discouraged from entering court proceedings due to them often being long,

[1849] Case of *Handyside v. the United Kingdom*, Application No. 5493/72, Judgment, ECHR, 7 December 1976, para. 49.
[1850] Case of Erkaban v Turkey, Application No. 59405/00, Judgment, ECHR, 6 July 2006, para. 56.

expensive and uncertain and due to lack of legislative knowledge.[1851] Although the Article 54a of the Criminal Code of Serbia does introduce the definition of hate crime on the grounds of race, religion, nationality, ethnicity, gender, sexual orientation or gender identity of another person, hate speech does not necessarily have to be a crime and therefore it cannot be treated as a synonym for hate crime. Article 75 of the Law on Public Information and Media forbids encouragement of discrimination, hatred or violence against a person or group of persons because of their belonging or non-belonging to a race, religion, nation, sex, because of their sexual determination or other personal characteristics via ideas, opinions, or information published in the media. Commissioner for the Protection of Equality has found a violation of Article 11 of the Anti-discrimination Law due in the case of P.P v A.T, for posting (and failing to remove) hateful speech based on sexual discrimination on Facebook, which then went on to encourage hatred, violence and discrimination among the commentators of said post.

Progress report on Serbia in the EU accession process for 2018 provides some insight, providing that hateful and discriminatory speech is often tolerated in the media and that both judicial and prosecuting authorities rarely respond to such cases.[1852]

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

In the Republic of Serbia the main mechanism for blocking and taking down internet content is regulated by Article 20 of Law on electronic commerce.[1853] It is conducted on court orders by a provider of information society service. As is the case in the majority of European countries, regulation is limited in this area. The law does not instruct the providers on how to act if there is no court order. In many European countries this legal gap is filled by self-regulation by the private sector. For self-regulation to be effective there ought to be relevant organisations of private entities in a certain field that will create regulation needed. In the Republic of Serbia activity of such organisations is limited, for e.g. The Association of ISPs of Serbia does not have a working website.[1854] Efforts were made by media organisations such as the Press Council by creating

[1851] Predrag M. Nikolić, Govor mržnje u internet komunikaciji u Srbiji, University of Belgrade, Faculty of Political Sciences, Belgrade, 2018, page 111.

[1852] Commission Staff Working Document, Serbia 2018 Report, European Commission, Strasbourg, 2018, page 26.

[1853] Sluzbeni glasnik RS;, br. 41/2009, 95/2013 i 52/2019.

[1854] http://www.uisp.rs/index.php?option=com_comprofiler&task=userprofile&user=152

'Guidelines for implementation of Journalists' Code of Ethics in the online environment'[1855] which aid journalists and news outlets in the online environment.

4.1. Are there any safeguards in place for ensuring the protection of freedom of expression online where self-regulation is applied?

The document that seeks to protect freedom of expression online is 'Declaration on respect of internet freedom in political communication'[1856] initiated by Share Foundation which was signed by some of the major media outlets and internet related associations in Serbia. The Declaration states in paragraph 1 that it is illegal to forcefully remove and block access to internet content. It is created as a guideline for application of regulation prescribed by the law. It also encourages the public to report violations of its rules. Reported violations are forwarded to government bodies or Press Council for further examination.

4.2. Which particular models are applied, e.g. a right to repost after notice and take down, or a right to be noticed of a takedown request and to object to the same?

In 'Guidelines for implementation on Journalists Code of Ethics in the online environment' created by Press Council it is recommended that the online media and online publications, in accordance with their technical capacities, develop a system of notice of users on why certain user generated content was not published in case of pre-moderation, or why certain user generated content was removed if post-moderation is applied. Effectiveness of these guidelines, or lack of it, can be seen in a study done by Press Council 'Analysis of implementation of Guidelines for implementation on Journalists Code of Ethics in the online environment in 70 media'[1857] where it was found that out of 70 media, 18 did not allow commenting at all.

Out of 52 that allowed, 32 had rules for commenting, 20 did not. In the same study it was found that the majority of media that allowed commenting (49 media outlets) applied the system of pre-moderation and only tree applied limited post-moderation.

Rules for posting comments, where the rules are public, in the majority of cases have a clause that publishers will keep the right to arbitrarily choose the

[1855] http://www.savetzastampu.rs/latinica/smernice-za-primenu-kodeksa-novinara-srbije-u-onlajn-okruzenju

[1856] https://deklaracija.net/

[1857] Savez za štampu <http://www.savetzastampu.rs/doc/szs-analiza-primene-smernica-prirucnik.pdf> February 2018.

comments allowed, with some news outlets even keeping the right to alternate the content of comments posted, for e.g. Informer.[1858] Prevalence of strict pre-moderation mechanisms can be attributed to the practice of Serbian courts. In 'Guide for good practice and regulatory models for responsible posting of online comments'[1859] created by Share Foundation, it is stated that courts in Republic of Serbia have taken a stance that the publisher of online media shares the responsibility for comments posted on their platforms which, as the authors assess, encourages limiting of online freedom of speech. In cases of web hosting, all major web hosts in Serbia in their terms[1860] of use state that the company is reserving the right to remove any content it assesses as inappropriate without an obligation to notify the user, or to give a justification for the removal. Legality of this clause can be questioned, as Law on public information and media[1861] states in article 4: 'Freedom of public information must not be violated by … influence on or control of … networks of electronic communications which are used for distribution of media content.'

4.3. Is there a grievance redressal mechanism available? If yes, are they sufficient/appropriate?

The Press Council has formed a Press Complaint Commission. The Commission is made up of journalists, members of journalist associations and members of the civil society. Commission decides on complaints on violations of Code of journalists which includes online media content. The drawback of this grievance redressal mechanism is its limitation to the sphere of press. There are no grievance redressal mechanisms where self-regulation is applied in the area of web hosting. This lack of self-regulation allows internet providers to freely decide on which content they will publish, but also it opens a path to third-party influence, as internet providers bear no responsibility for censoring content on websites it hosts.

1858 Informer < https://informer.rs/pravila-koriscenja >

1859 ShareFoundation<https://resursi.sharefoundation.info/wp-content/uploads/2018/10/vodic-pravni_ii_web.pdf > 2015.

1860 Unlimited Terms of Use<https://unlimited.rs/uslovi-koriscenja-tos/>, Adria Host Terms and Conditions <https://adriahost.rs/pravilnik/ >

1861 Sluzbeni. glasnik , no. 83/2014, 58/2015, 12/2016.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

5.1. Please identify specific legislation on the issue as well as related jurisprudence and decisions of competent authorities.

The answer is affirmative, however, since the Republic of Serbia is not a member state of the European Union, we need to take a look at differences between the General Data Protection Regulation and the Serbian Version of it. Before that, it would be conceivable to give a small introduction about implementation of Law on Data Protection in Serbia, General Data Protection Regulation itself and Right to be Forgotten in general, in order to hollow out and develop research straight into problems and possible lack of that right.

A new Law on Data Protection[1862] (in the following text the term Law shall be used) in the Republic of Serbia was adopted in November 2018 and with a delay of nine months, in August 2019, came into force. Text of the Law is for the most part an adapted translation of the GDPR and, as much as possible, harmonised with the current standards of the relevant documents of the European Union related to the data protection, as a result of the international obligation defined by the 2008 Accession Agreement[1863] as a candidate for EU membership. Further is made clear in Report of European Commission that new Law is necessary on that subject.[1864] For the occasion of implementing the Law taken into account is the fact that Republic of Serbia is non-member of the EU, which means that the GDPR cannot be directly applied. Secondly, Serbian legal system has certain differences compared to member states' jurisdiction, so it is impossible to take all provisions as such, without adjustment of the Law.

On the other hand, there is, according to the words of Commissioner for Free Access to Information of Public Importance and Personal Data Protection (in the following text just - Commissioner), an attained level of awareness of the protection of personal data and rare applications of regulations in this area are one reason more why Serbia has to work hard to get protection on EU level. [1865]

[1862] Zakon o zaštiti podataka o ličnosti, "Sl. Glasnik RS", br. 87/2018.

[1863] Ministry of Finance of the Republic of Serbia|mfa.gov.rs |<http://www.mfa.gov.rs/en/foreign-policy/eu/political-relations-between-the-republic-of-serbia-and-the-european-union/12452-chronology-of-relations-between-the-republic-of-serbia-and-the-european-union>

[1864] European Commission|Serbia2016 Report <https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_serbia.pdf>, Page 61.

[1865] Rodoljub Šabić, ex Commissioner, in interview on netokracija.rs/gdpr-definicija-uredba-136384;

The numerous shortcomings of the new Law on Personal Data Protection, in particular the ones that refer to unclear provisions and overwritten mechanisms that do not exist in the domestic legal system, are leading to question its applicability. However, it is important to note that this Law, even if only normative, is the highest standard for the protection of personal data. Sooner or later, there will be shortcomings and gaps resolved by subsequent interventions, amendments etc., while significant legal innovations remain embedded in our system of human rights protection.[1866] With the opportunity to interpret the domestic law, in particular - Law on Personal Data Protection, GDPR and its Preamble will be used as a way to apply European regulation, and within all intentions, which are expressed in the Preamble, starting with the confirmation that protection of personal data is one of the fundamental human rights. The way GDPR standards are interpreted should be a guideline for the interpretation of Serbian Law as well. An integral part of the new European regulation, the Preamble[1867] consists of as many as 173 points - recitals which further elaborate legal norms and clarify the purpose of all GDPR provisions, starting with point 1, which defines the protection of personal data as a fundamental human right. The Preamble is therefore not only useful but already a necessary starting point for interpreting regulations. The domestic law did not transpose the GDPR Preamble, however its presence on the occasion of the interpretation does not come into question.

The vast majority of the provisions of the Law follow GDPR and are in conformity with its provisions. Although the current law is insufficient with regards to sanctions and criteria for sanctioning.[1868] All enterprises could use this advantage of harmonisation with EU to set up same provisions and use contractual clauses adopted by the European Commission, or documents that are already in practice[1869] that would ensure their transfer from EU to Serbia and onwards.

As was already mentioned, Right to be Forgotten is implemented in Article 17 GDPR and in Serbian Law discreetly in Article 30.

1866 Share Foundation| Vodič kroz zakon o zaštiti podataka o ličnosti i GDPR <https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf>

1867 Intersoft Consulting |April 27th 2016<https://gdpr-info.eu/recitals/ >

1868 TAIEX mission 30066, Assessment of the Draft Law on Personal Data Protection of Serbia; Desk stuy; Ljubljna 28 May 2019, Sironič Mater, Novak Anže https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/engEKStudija.pdf

1869 Muster zur Umsetzung der DSGVO in der Praxis, Vorlagen, Checklisten, Formulare, 2019; Feiler, Rainer Schmitt; Verlag Österreich.

The ight to be Forgotten has been in existence subject to comprehensive scientific discussions since it was derived by Mayer Schönberger.[1870] The key question is whether a person can force the world in the digital age to forget them. On the other hand, one often hears that the internet 'forgets nothing', or that intended data is not deleted or is not possible in the program. Even before the GDPR came into force, the "Right to be Forgotten" or "Right to Delete" in one decision of the Court of Justice of the European Union (CJEU), directed against Google, received special media attention. It is interesting that the CJEU itself did not use the two terms in its decision. [1871]

The Court of Justice of the European Union interprets the law Union, ensuring uniform application of the law in all Member States. In Accordance with its mandate, the Court has, over the years, made a number of decisions that have played a significant role in the interpretation and application of data protection standards. One of the most well – known Court decisions in the area of relationships in the online sphere, certainly is in the case of Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez[1872] , which in 2014 established the so- called the Right to be Forgotten. The GDPR then incorporated this right into the regulatory corps of protection. On the other hand, the ECJ only considers interest in public information. Freedom of expression and freedom of the press remain unmentioned.[1873] Regulations regarding such a conflict fundamental rights fall under the jurisdiction of the national legislature under Article 85. The determination is so abstract and vague that this is precisely the one crucial point about the Right to be Forgotten where considerable divergences of interpretation are to be expected.

Right to be forgotten or right to delete in Serbia:

As was already mentioned, it is stipulated in Article 30. Model for such an instrument was Article 17 GDPR. Even with translation and adaptation there are small differences that imply a diversity of legal systems.

First of all, Article 30 follows the time construction in English language version (have unlawfully processed). That means that the fact of paragraph 1 is only fulfilled if the state of illegality persists. If the originally illegal state is now legal,

[1870] Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht 2:105 -109, S 107.
[1871] 8. Datenschutzrecht (Spring) 1. Aufl; September 2018, Lexis Nexis, S 124.
[1872] C-131/12 - Google Spain und Google.
[1873] See Article 11 of Charter of Fundamental Rights of the European Union.

there is none for teleological reasons to grant a right to cancellation, as it was penalised. [1874]

The term 'Right to be Forgotten' is misleading because it is personal data according to Law not as it were with an expiry date, but rather just a right granted on deletion under the conditions specified in Article 30. Compared to Article 17 GDPR there is no term Right to be Forgotten as well, even not in quotation marks, how it is in GDPR, which probably refers to underlying legal policy discussion.

Furthermore, paragraph 4 stipulates that data subject shall submit the request for erasure to the controller. Such provision is not included in GDPR Article 17.[1875] It is not clear why such a provision is required. The provision should not affect the obligation of the processor to assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to request for exercising the data subject's rights (when for example data subject would file his request to exercise his rights with the processor). If the processor could lawfully refuse to act upon receiving a request for erasure, by stating that data subject should according to Article 30 paragraph 4 of the Law submit the request for erasure to the controller – in this case, such exception would be in contradiction to the purpose set by the GDPR. [1876]

Article 30 of the Law refers to the right to delete personal data, the obligation the operator to delete the data that he or she is processing, so the law must also regulate the way in which the controller acts, the way in which data is deleted when it comes to automatic and non-automatic processing, bearing in mind that the action of deleting data in a non-digital form actually means destroying the data. [1877]

However, it should be noted that since the Republic of Serbia is not yet an EU member, this judgment does not apply to our citizens and Google has no obligation to act on claims for Right to be Forgotten if the request comes from Serbia.

There is no case law on such instruments yet in Serbia.

[1874] Feiler in Feiler/ Forgo in Art 17 Rz 5; EU- DSGVO; Verlag Österreich.

[1875] Unlimited Terms of Use<https://unlimited.rs/uslovi-koriscenja-tos/>, Adria Host Terms and Conditions <https://adriahost.rs/pravilnik/ >

[1876] ibid.

[1877] Zaštita podataka o ličnosti: stavovi i mišljenja Poverenika, Beograd 2019, <https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/Publikacija4ZZPL/4PublikacijaZZPL.pdf>

How to claim rights regarding the processing of personal data?

Request for access, correction and amendment, deletion, restriction of processing, data portability, interruption of processing as well as non-application of the decision made on the basis of automated processing. The person whose data is being processed, data subject, is submitted to the controller. If the controller, in accordance with Article 21 paragraph 3 of the Law, justifiably suspects the identity of the person who submitted the request, it may require the person to provide additional information necessary to confirm the identity, in accordance with Article 5 paragraph 1 item 3 of the Law. Article 5 of the Law, interpreted in accordance with Article 5 GDPR, implies legitimacy of the purposes in line with other legal obligations as they are derive in particular from labour law, contract law or the consumer protection law. [1878]

The controller is obliged to provide a copy of the data processed by the person to whom the data relates to his request. If the request for a copy is submitted electronically, the information shall be provided in the commonly used electronic format, unless the data subject has requested it to be otherwise provided. If the data subject requires the making of additional copies, the controller may require reimbursement of the necessary expenses for the same.

When is the complaint filed with the Commissioner?

If the controller fails to act on the request of the data subject, he or she shall inform the person without delay of the reasons for non-compliance, not later than within 30 days from the day of receipt of the request, as well as of the right to file a complaint with the Commissioner or suit to the court.[1879]

6. How does your country regulate the liability of internet intermediaries?

Internet intermediaries have a strong impact on the way we are practicing our rights and the way we interact. This term refers to internet providers that are primarily for-profit companies that have a job to connect users to the internet service as well as providing hosting, VPS, Cloud, registration of domain etc. They are also allowing us to connect to social media platforms, enable the processing of information and data, search engines, providers and store web-based services and to perform other intermediary functions. As we can see

[1878] see Article 29 Data Protection Working Party, Opinion 03/2012 on purpose limitation, WP203 [2013] 20 at http://ec.europa.eu/justice/data-protection/article 29/documentation/opinion-recommendation/ files / 2013 / wp203 en.pdf

[1879] https://www.poverenik.rs/sr-yu/za%C5%A1tita-podataka/s-prava-zp.html

usually they are not only providing internet service, but they are a complex system of services.

But they also search for, identify and remove allegedly illegal content and are required to assess the validity of requests from public or private parties to remove certain content, on the basis of: official requests from public authorities, internal content management policies, (often insufficient) regulatory framework, informal cooperation agreements with public authorities.

Because our lives in the 21st century are happening both online and offline, we need a system of protection of human rights online. The Internet cannot be a lawless place. And that is why internet intermediaries have a really important role in providing protection of human rights. One of the greater achievements of humanity such as free speech or abolition of racism, would not have been possible if there had been no system of regulating free speech online. However, this can also lead to abuse of blocking and taking down rights.

The internet and social networks are one of the best ways for people to connect today. In 2018. the average time spent on social networks was projected as 144 minutes a day which makes it an increase of 1 hour a day or 62.5% a day from 2012. [1880] All of these increases make it even more important to safeguard human rights online. It is primarily the obligation of states to make sure that laws, regulations and policies applicable to internet intermediaries effectively safeguard the human rights and fundamental freedoms of users. At the same time and in line with the UN Guiding Principles on Business and Human Rights, internet intermediaries have the responsibility to respect the internationally recognised human rights of their users and third parties affected by their activities. States and intermediaries therefore have to work together.[1881]

As one of the foundations of state power is the control of information, this was challenged by the borderless nature of the Internet and by the free flow of information across countries around the globe without respecting national laws. [1882]

The expansion of the human rights instruments has influenced the liability of internet intermediaries in two ways. Firstly, those instruments oblige courts to take account of claimants' rights in ways that sometimes require remedies to be conferred, reshaped or expanded. Secondly, those instruments recognise the rights and freedoms of intermediaries and their users in the ways that sometimes

[1880] Broad Band Search|<https://www.broadbandsearch.net/blog/average-daily-time-on-social-media>
[1881] Council of Europe|Roles and Responsibilities of Internet Intermediaries <https://rm.coe.int/leaflet-internet-intermediaries-en/168089e572>
[1882] OSCE <https://www.osce.org/netfreedom-guidebook?download=true>

place limits on the remedies available to the claimants or require a balancing exercise to be undertaken.[1883] In the Republic of Serbia, the main instruments are Constitutional Law, Law on Electronic Communication and European Convention on Human Rights.

The Constitution of the Republic of Serbia proclaims in Article 50, paragraph 3 that :'Competent court may prevent the dissemination of information through means of public informing only when this is necessary in a democratic society to prevent inciting to violent overthrow of the system established by the Constitution or to prevent violation of territorial integrity of the Republic of Serbia, to prevent propagation of war or instigation to direct violence, or to prevent advocacy of racial, ethnic or religious hatred enticing discrimination, hostility or violence.'

And in paragraph 4: 'The law shall regulate the exercise of right to correct false, incomplete or inaccurately imparted information resulting in violation of rights or interests of any person, and the right to react to communicated information.'

Law on Electronic Communication in Article 124 proclaims:

'In order to ensure the security and integrity of public communications networks and services, confidentiality of communications, and protection of personal, traffic and location data, the operator shall take adequate technical and organisational measures, suitable for the existing risks, and in particular measures for the prevention and minimisation of the effects of security incidents on users and interconnected networks, as well as measures for ensuring the continuity of operation of public communications networks and services. If the operator provides the service using some other operator's electronic communications network, associated facilities or services, it shall cooperate with that operator to ensure the security and integrity of public communications networks and services. In case of a particular risk related to the violation of the security and integrity of public communications networks and services (unauthorised access, significant loss of data, violation of the confidentiality of communications, personal data security, etc.), the operator shall inform subscribers of such risk and, in case the risk lies outside the scope of measures to be taken by the operator, of possible means of protection and costs related to the implementation of these measures.'

Besides Article 10 of European Convention on Human Rights[1884], in Serbian law system there is no liability for blocking and taking down content that is against

[1883] Jaani Riordan, "The liability of Internet Intermediaries", Oxford, United Kingdom : Oxford University Press 2016.

[1884] <https://www.echr.coe.int/Documents/Convention_ENG.pdf>

fundamental freedoms. But the majority of the internet intermediaries' general business conditions are regulating the illicit behaviour of the internet users. However, it isn't written that it will be taken down, just that the user is liable to internet intermediaries for material and non-material damage caused by itself.

Following text represents general conditions of the biggest internet intermediary in Serbia, SBB:

The behaviour of the Subscriber shall be considered inadmissible if it is contrary to the imperative regulations of the Republic of Serbia and international law or to the treaties, conventions, and recommendations relating to the use of the Internet, computers and computer networks, as well as the rules and instructions defined in the 'Acceptable Internet Usage Policy' And 'Internet Technical Specifications' at www.sbb.rs under 'Customer Service - General Documents.' Behaviour of the Subscriber shall be considered inadmissible, especially if it commits a criminal offense or an economic offense, violates the provisions of copyright and industrial and intellectual property rights, commits an act of unfair competition if it threatens or violates one's rights if it violates good business practices and consumer protection rules if they violate contracts, conventions, and recommendations in the field of telecommunications law. Some of the behaviours that are considered illegal are:

- Use of the service, and the ie selected option of SBB cable Internet service for unauthorised access or for obtaining control over other systems on the local network and the Internet;
- Endangering the uninterrupted use of the service by other users
- Endangering the smooth operation of the SBB network or any other part of the Internet;
- Distribution of malicious content, viruses or other programs with destructive features;
- Breaking the privacy of other SBB cable Internet subscribers or the Internet in general;
- Unauthorised modification of the modem's default IP address or MAC address;
- Distribution of unsolicited e-mails via email or Usenet conferences (spam). '

Since the Republic of Serbia is a signatory of European Convention, precedents of European Court for Human Rights are our sources of law as well. The most famous case is DELFI v ESTONIA. Judges there said: 'The importance of the role of intermediaries should be underlined. They offer alternative and

complementary means or channels for the dissemination of media content, thus broadening outreach and enhancing effectiveness in the media's achievements of its purposes and objectives. In a competitive intermediaries and auxiliaries market, they may significantly reduce the risk of interference by authorities. However, given the degree to which media have to rely on them in the new ecosystem, there is also a risk of censorship operated through intermediaries and auxiliaries. Certain situations may also pose a risk of private censorship (by intermediaries and auxiliaries in respect of media to which they provide services or content they carry).' The importance of internet intermediaries is implicated as a tool for achieving democratic Freedom of Expression online, because they are providing access to valuable information.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Regarding these topics, it is hard to make any predictions since there is no debate in the National Assembly of Serbia on these issues and there aren't any proposals for legislation in this area. There is also no initiative by the media in this regard. On the other hand, the experts are warning that in the media and on the internet there are acts contrary to private interests (publication of crime victim photos, disregard for the presumption of innocence) and the public interest (obstruction of the official investigation, criminal proceedings). They suggest that appropriate legislative measures should be taken to sanction and reduce such actions in the future.

The most recent violation of the victim's privacy happened when tabloids published pictures of a girl in an ambulance car, moments after she was rescued from the place where the kidnaper was holding her. Before the girl's rescue, the same tabloids also published a testimonial of the kidnapper that he gave after committing a previous similar crime in the past. This testimonial gave full details of the torture he committed. Belgrade Centre for Human Rights filed criminal charges against N.N suspect from either the prosecutor's office or police officer who allegedly sold the information to the tabloids. [1885]

As a candidate for membership in the European Union, legislation of the Republic of Serbia should harmonise its legislation with EU law and come closer

[1885] 'Podneta krivična prijava zbog objavljivanja iskaza 'Malčanskog berberina' u tabloidima', Južne vesti, 12. January 2020.

to all EU Standards. It is our opinion that the process of harmonisation will go slow. So far, there haven't been many initiatives or efforts to make things go faster. On many subjects in different areas Serbian legislation preserves the status quo. For the Right to be forgotten to be in use such as it is in the EU, an option to use this right as an instrument needs to be obtained at first member-state. Secondly, public opinion on that subject must be on a higher level, for it to be the foundation stone of further way. To expect such actions in 5 years could be pretentious, but on the other hand reasonable term. In the end, one of the most difficult factors which matter is the unpredictable political situation in Serbia and as long political courses and the winds blow towards the EU, there shouldn't be worry about it.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

The Constitution of the Republic of Serbia prescribes freedom of thought and expression in Article 46. In Serbian legislation there are several more laws which regulate Freedom of Expression in online environments and hate speech in online environments. According to The Law on Electronic Media, the obligation to respect human rights Article 50 'Media service is provided in a way that respects human rights and in particular the dignity of the individual. The Regulator shall ensure that all programs content respects the dignity of individual and human rights and in particular takes care not to show degrading treatment and scenes of violence and torture, unless there is programmatic and artistic justification. Content that may impair the physical, mental or moral development of the minor must be clearly labelled and not published at a time when the minor may reasonably be expected to accompany them, given the usual schedule of their activities, except exceptionally as a protected conditional access service in a manner provided for by this law.' According to the same law, Article 51: 'The Regulator shall ensure that the program content of the social media service provider does not contain information that encourages, in an open or covert manner, discrimination, heated or violence on the basis of race, colour, ancestry, citizenship, nationality, language, religious or political beliefs, gender, gender identity, sexual orientation, property status, birth, generic characteristics, health status, disability, marital and family status, conviction, age, appearance, membership in political, trade union and other organisations and other real or assumed personal characteristic.'

Hate speech is also defined in the Anti-discrimination Law in Article 11. These are listed the most relevant regulations of national legislation.'

Observing Article 10 of the European Convention on Human Rights and Article 46 of the Constitution of the Republic of Serbia we can conclude that boundaries of Freedom of Expression have been set quite wide. However, the Republic of Serbia defines the question of Freedom of Expression only in the Constitution. The Law of Electronic Media does not mention explicitly freedom of expression, it only mentions bans on hate speech in Article 51. Practically, Freedom of Expression online is not defined in the Law on Electronic Media. Based on that, we can conclude that it is much more important to underline things that are forbidden, than to stress things that cover the area of rights. It is a fact that people are more aware of things that are forbidden and it is easier to understand right through limitations of the right.

In this modern age, the need for control is omnipresent, we can put it along with the need for power and only then we will be able to understand why we cannot just live a simple life without any boundaries and censorships. Censorship is way to control others, to control what you can and what you cannot, what you know and what you do not know, it is not only about hate speech and ban of hate speech in the aim to be more tolerant and open our sights in every single way and not hurting anyone by telling some mean words. It is about power and it always has been. Through history, we have had the opportunity to see that winners are the ones who write it.

Censorship is good, as well as everything that stops people and sets boundaries, because people simply are not able to set boundaries to themselves, but at the moment when people start to set boundaries it is hard to know when to stop.

In the Law on Electronic Media of the Republic of Serbia the Regulator is the body which ensures that online content does not contain any hate speech. The Regulator has the right to impose sanctions on those who use hate speech in the media. In the theory it looks nice, but it is pretty different in the practice. The Regulator should be the body which ensures that online content does not contain any hate speech, but in the cases where the Regulator had the role to solve the case it wasn't as expected. In the cases where online content obviously contained hate speech, the Regulator gave just the warning measure, no penalty, just warning measure. Hate speech is a really big problem and it gives a bad example, so it must disappear. And the Regulator should act, supervise and monitor more strictly for better results.

There is a tiny line between allowing Freedom of Expression online and protecting against hate speech in an online environment. For sure, there are

misunderstandings and misconceptions especially about allowing freedom of speech online, because the words which are used can be misinterpreted and sometimes it can be interpreted in an offensive way, even if they are not meant to be offensive. The case is different when talking about hate speech in online environment, everybody can recognise hate speech, especially because in every person there is a sense for moral and immoral and people do not have to be educated, they do not have to be certain age or have massive experience while recognising hate speech, there is moral in kids, men and women, no matter to age, gender, nationality, race, religious or political beliefs… To sum up, it is really hard to be completely sure that there is no violation of anybody's right and that balance is present. In the Republic of Serbia, with the fact that the definition of freedom of speech online has been left out, a certain adequate balance is highly unlikely present. Of course, the aim of legislation in every country is to bring perfect equilibrium to what is allowed and what's not allowed and to sanction those who do not respect law. Also, with the fact that online is such a big space that covers mostly all countries in the World it is hard for one country to ensure adequate balance between Freedom of Expression online and protecting against hate speech in online environment, we have to face it that we are small creatures and sometimes it is beyond our countries' possibilities.

The things that should be done to reach balance between Freedom of Expression online and protecting against hate speech in online environment are: national legislation should contain international and regional standards which promote Freedom of Expression and equality and outline the need for fight the hate speech; 'they should ensure that the national law allows for the effective prosecution of illegal online hate speech in conformity with the case law of the European Court of Human Rights, while fully respecting Freedom of Expression; they should also ensure that national legislation covers all forms of online incitement to violence against a person or a group of persons, bullying, harassment, threats and stalking, so that these can be effectively prosecuted under national law.' When all these things are accomplished, the Republic of Serbia will reach an adequate balance between allowing Freedom of Expression online and protecting against hate speech in an online environment.[1886]

[1886] Council of Europe, Links between freedom of expression and other human rights, <https://rm.coe.int/liberte-d-expression-guide-to-good-and-promising-practices-and-analysi/168098f553>%20accessed%2017%20February%202020.>;accessed 17 February 2020.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

When it comes to allowing freedom of expression online, it can be noted that Freedom of Expression is guaranteed in the Constitution, as well as many other laws, as a general clause. Proceeding those clauses are the ones that set restrictions that mostly involve the right to privacy, protection of public interest, minors' rights, prohibition of discrimination etc.

As an example, we are going to analyse a case to which the authorities reacted and prosecuted some of the newspaper publishers that made public information that were confidential due to the fact that the criminal investigation was still in progress at the time. The situation was especially delicate since the victim was a minor and the newspaper publishers wrote parts that completely matched the testimony she gave to the police and the public prosecutor. All that led to the conclusion that someone 'leaked' this information and endangered the minor's right to privacy. This criminal procedure is still ongoing, the court is yet to express its attitude in this particular case.

On the other hand, there have been cases in which the court considered the perpetrators did not endanger the public order and the public interest enough to be criminally prosecuted, so the Freedom of Expression was not limited in any way. In 2018 Dragana Rakić, a librarian that also writes columns for newspapers published on her Facebook account a statement 'Aleksandar Čupić is the largest journalistic scum'.[1887] Čupić considered that she insulted him and therefore committed a criminal offense. The court decided that the statement was not an insult but a value judgement, and liberated her of any criminal liability. The legal basis was the Constitution of the Republic of Serbia and the European Convention on Human Rights that provide the Freedom of Expression.

In general, the conclusion would be that, analysing the legislation, the Republic of Serbia set some very good limitations to the Freedom of Expression. They all involve protections of other freedoms and rights guaranteed by the Constitution and the European Convention on Human Rights. However, there is always room for improvement when it comes to the enforcement of the law.

[1887] < https://www.cenzolovka.rs/tag/dragana-rakic/>

10. How do you rank the access to freedom of expression online in your country?

Considering everything written in this legal research, we can say that Freedom of Expression online in Serbia is positioned very well –We would rank it with grade 4. But this is said by considering the Serbian laws. But is it really this top 4 rating reality?

The Non-government Organisation named Freedom House, wrote in their annual report for 2019[1888] that Serbia's status declined from Free to Partly Free due to the worsening conditions under which the elections are being held, but also the attacks on independent journalists. Here is the most important citation from that report: 'Despite a constitution that guarantees freedom of the press and a penal code that does not treat libel as a criminal offense, media freedom is undermined by the threat of lawsuits or criminal charges against journalists for other offenses, lack of transparency in media ownership, editorial pressure from politicians and politically connected media owners, and high rates of self-censorship.'

As we can see, legally, only things that are really forbidden are essentials for functioning of the modern society in the 21st century such as hate speech, intolerance against race, nation etc.

But in reality, circumstances are much different. We are all witnesses that democracy is today being used for adverse purposes. In Serbia, the current government is using the side ways to cover the evidence about illegal happenings related to their political party. And they will try to cover the truth at any cost. Writing content against the ruling party can get you fired or you can get you brought to the police hearing.

The situation could be explained by one extreme example which happened recently to a Serbian journalist.

The most recent brutal attack on a journalist happened in December 2018 when the house of journalist Milan Jovanović was set on fire, while he and his wife were inside.[1889] The attackers wanted to block them from going out by shooting at the house, but they managed to escape through a window and left not heavily hurt. Mr. Jovanović started writing in 2012, working on stories that involved local municipality authorities and their criminal behaviour, corruption, and financial malversations. Before writing he spent 30 years working in police as an

[1888] <https://freedomhouse.org/country/serbia/freedom-world/2019>

[1889] 'Serbia: Journalist Milan Jovanović attacked with Molotov cocktail', International Federation of Journalists, 18 December 2018.

operative and shift manager at Utility operating centre. At the age of 69, he was left homeless but inspiringly still willing to pursue the truth.

The ruling party tried to stand by the people who were most probably behind the attack, but since the story went viral and it was impossible to cover it up, the former president of Grocka municipality Dragoljub Simonović was accused of instructing others to set the house of the journalist on fire. In July of 2019 trial was moved again for September because none of the three accused showed up and their lawyers said they did not know why. One of the lawyers also did not show up and when on the same day he was asked about it, he said he considered the ongoing press conference more important than the specific case. The press conference was organised in support of the chamber of lawyers whose member was killed in the summer of 2018, a year before. All three accused were fined for missing the trial that day. Mr. Jovanović, who is under police protection, says he believes this is a classic case of obstruction of justice and that it is not in any way reasonable for accused to not be in custody (as if there was no threat), and for him to be under protection at the same time.[1890]

The trial was again moved for November and then again for December because one of the accused did not show up. In the meantime, Mr. Jovanović said the obstruction of justice continues and that lawyers of the accused are pressuring witnesses to say in their testimonies they were pressured by the police when they first spoke to them on the ground, which would lead to the inadmissibility of their first testimonies. A year after, the journalist's house is still not in good shape. Some rooms were renovated but he still needs resources such as furniture and other joinery. He received a donation of around 23000USD from the Slavko Ćuruvija foundation, which gathered money donations from people. UNS and NUNS, both domestic journalist associations also contributed. Neither municipality nor city offered to help him. Seven months after the attack he met with Prime Minister Ana Brnabić in a reception in the French embassy, where she promised to help him if he contacted her. In August they spoke and she promised to help the repair of the house and also said she will put her focus on anything the budgetary inspection finds, regarding the corruption he wrote about. This is an ongoing case that will hopefully start its unrevealing after the latest hearing scheduled for February 14th.

As we can see above, journalists in the Republic of Serbia are not in the greatest position currently. Even European Union's

[1890] Interview for N1 TV broadcaster, 26 July 2019.

researchers warned Serbian government that in Brussels, they are aware of the exchange of messages between the Organization for Security and Co-operation in Europe (OSCE) and the Serbian Government on what they say from the OSCE, worrying trend of censorship on the internet in Serbia. [1891]

Recent case of the influence on journalists is that during the COVID-19 lockdown in Serbia, it happened that journalist Ana Lalić published a newspaper article[1892] about medical workers that do not have enough of the basic equipment and have poor working conditions at the time of the pandemic at the Clinical Center of Vojvodina in Novi Sad. After publishing that article she was detained and ordered to be detained by the police for 48 hours on suspicion that she could repeat the crime, publishing texts that will cause panic and riots. Her lawyer Srđan Kovačević said that there was no hearing, but that they only handed a decision to her. Nova.rs journalist Ana Lalić is this year's laureate for the Deutsche Welle Freedom of Speech Award. 'They represent all journalists around the world who have disappeared or been arrested or are in danger of reporting on the COVID-19 pandemic, 'DW said. Lalić later said that on April 20, doctors and experts 'close to the Government' admitted that there was not enough equipment at the beginning of the epidemic.

There are more examples to these smearing campaigns and other forms of pressure. As we could see in this paper, legally speaking there is almost complete freedom of reporting, but in practice it cannot be said. There are a large number of journalists who are afraid for themselves and their families and therefore choose not to report on matters related to the government. We believe that this is a problem of the whole society and we hope that it will be solved in the future.

11. How do you overall assess the legal situation in your country regarding internet censorship?

The Republic of Serbia is one of the countries that has no specific legislation on the issue of Freedom of Expression on the internet. In the absence of a specific or targeted legal framework, the Republic of Serbia relies on an existing general framework considering media freedom, freedom of speech, etc. These legislative acts prescribe limitations of these freedoms on the grounds of protecting rights and reputation of others, public health, authority and objectivity of the court, morals of democratic and national security.

[1891] https:/www.dw.com/hr/eu-upozorio-srbiju-zbog-cenzure-na-internetu/a-17681364 accessed 28th February, 2020th

[1892] <https://nova.rs/drustvo/kc-vojvodine-pred-pucanjem-bez-zastite-za-medicinske-sestre/ >

Internet intermediaries are held responsible for the content published online. Therefore, the Republic of Serbia gives permission to the state authorities to take down internet content or sanction in another acceptable way the ones responsible for crossing the limitations. Aside from the state authorities, the private sector has limited authorities in this matter. For example, Press Complaint Commission authorities are limited to the sphere of press.

As the state that tends toward becoming a member of the European Union, the Republic of Serbia will probably have to regulate questions regarding this matter, in order to reach the level of rights on the internet EU states have reached. However, for now, there are no motions inside or outside of the parliament for the regulation of this matter.

One of the reasons for this is the impossibility of the legislator to keep up with the pace of technology that develops rapidly. Another reason is that the legislation always follows social movements. In Serbian society Freedom of Expression on the internet is not a current topic.

With the full right one can ask how can exercising rights on the internet be an unpopular topic in the age of modern technology. The answer to the question is simple when we take into consideration the fact that only 60% of the country has access to the internet. In accordance with the plan of the Government of the Republic of Serbia, in the following three years appropriate measures are to be taken in order to provide internet access to all the citizens of the Republic of Serbia. Only after this plan is fulfilled, it could be expected that the topics such as Freedom of Expression on the internet become one of the ongoing questions in front of the legislative body of the Republic of Serbia.

Conclusion

As the use of the internet is continuously growing and its role in human communication is becoming more valuable than ever, we believe it is of utmost importance to have a well-developed regulation concerning it, including the questions of Freedom of Expression and censorship. The Internet should not be viewed as just another means of communication as it is in many cases fully substituting the role of real life. In the recent outbreak of the Coronavirus, it was shown that in cases of emergency it can be used for conducting the majority of the business. Such value of the internet is in our opinion still not fully appreciated by the general public.

For these reasons, we believe that it would be a responsible approach from the government to invest resources into better regulating the area.

The State does not regulate the blocking of internet content, and we believe it would be desirable to regulate this because from the publication of the disputed content until the taking down-damage has already been done.

Also, the regulator should implement a better monitoring system and we believe that should be daily supervision. Furthermore, sanctions should be more serious instead of only the imposition of a warning measure. In this regard, it would be great for the State to better regulate and define the case of when and how the regulator can act better and impose more effective sanctions.

Another important aspect would be the higher involvement of the private sector and the NGOs who are for now, as it was demonstrated in this report, also not investing sufficient effort into self-regulating or initiating regulation of censorship on the internet.

For these reasons it is our assessment that the current state of internet censorship in the Republic of Serbia cannot be judged as other areas of legislation as it is an area yet to be developed. This should open a path towards further research in the future when the role of the Internet becomes more of a focus point for the legislators.

Table of legislation

Title in Serbian language	**Corresponding translation in English**
Ustav Republike Srbije	The Constitution of the Republic of Serbia
Zakon o javnom informisanju i medijima	Act on Public Information and Media
Zakon o slobodnom pristupu informacijama od javnog značaja	The Act on free access to information of public importance
Zakon o elektronskim medijima	The Act on Electronic Media
Krivični Zakon	Criminal Code
Zakon o elektronskoj trgovini	Law on Electronic Commerce
Zakon o zaštiti podataka o ličnosti	Law on Personal Data Protection
Zakon o oglašavanju	Advertising Law
Zakon o radiodifuziji	Law on Radio Diffusion
Zakon o elektronskim medijima	Law on Electronic Media
Zakon o zabrani diskriminacije	Law on Prohibition of Discrimination
Zakon o zabrani manifestacija neonacističkih ili fašističkih organizacija i udruženja ili fašističkih simbola i obeležja	Law on the Prohibition of the Manifestation of Neo-Nazi or Fascist Organizations and Associations and Prohibition of use of Neo-Nazi or Fascist Symbols and Insignia

Bibliography

English titles

Reports

Final Report International Legal Research Group On Freedom of Expression And Protection Of Journalistic Sources

Commission Staff Working Document, Serbia 2018 Report, European Commission

Books

Steven Greer-The exceptions to Articles 8-11 of the European Convention on Human Rights

Jaani Riordan, "The liability of Internet Intermediaries", Oxford, United Kingdom

Digital resources

http://www.mfa.gov.rs/en/foreign-policy/eu/political-relations-between-the-republic-of-serbia-and-the-european-union/12452-chronology-of-relations-between-the-replic-of-serbia-and-the-european-union

https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_serbia.pdf

http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation / files / 2013 / wp203 en.pdf

https://www.broadbandsearch.net/blog/average-daily-time-on-social-media

https://rm.coe.int/leaflet-internet-intermediaries-en/168089e572

https://www.osce.org/netfreedom-guidebook?download=true

https://www.echr.coe.int/Documents/Convention_ENG.pdf

https://www.ifj.org/media-centre/news/detail/category/safety/article/serbia-journalist-milan-jovanovic-attacked-with-molotov-cocktail.html

Case law

Handyside v. United Kingdom App. no. 5493/72, (ECHR 7 th December 1976), page 49

Case of Handyside v. the United Kingdom, Application No. 5493/72, Judgment, ECHR

Case of Erkaban v Turkey, Application No. 59405/00, Judgment, ECHR

Google Spain SL and Google Inc. v Agencia Espanola de

Proteccion de Datos (AEPD) and Mario Costeja Gonzalez

Case of Delsi As v. Estonia

Serbian titles

Legislation

Zakon o elektronskoj trgovini 'Službeni glasnik Republike Srbije' br. 41/2009, 95/2013 52/2019

Zakon o javnim informacijama i medijima 'Službeni glasnik Republike Srbije' br. 83/2014, 58/2015, 12/2016

Zakon o zaštiti podataka o ličnosti, "Sl. Glasnik RS", br. 87/2018

Books

Predrag Dimitrijević, Jelena Vučković- Analiza medijskog zakonodavstva u Republici Srbiji

Predrag M. Nikolić, Govor mržnje u internet komunikaciji u Srbiji, University of Belgrade, Faculty of Political Sciences, Belgrade, 2018, page 111.

Digital resources

http://www.uisp.rs/index.php?option=com_comprofiler&task=userprofile&user=152

http://www.savetzastampu.rs/latinica/smernice-za-primenu-kodeksa-novinara-srbije-u-onlajn-okruzenju

https://deklaracija.net/

http://www.savetzastampu.rs/doc/szs-analiza-primene-smernica-prirucnik.pdf

https://informer.rs/pravila-koriscenja

https://resursi.sharefoundation.info/wp-content/uploads/2018/10/vodic-pravni_ii_web.pdf

https://unlimited.rs/uslovi-koriscenja-tos/, https://adriahost.rs/pravilnik/

https://www.netokracija.rs/gdpr-definicija-uredba-136384

https://sbb.rs/Binary/30847/Opsti-uslovi.pdf

https://www.sharefoundation.info/Documents/vodic_zzpl_gdpr_share_2019.pdf

https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/engEKStudija.pdf

https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/Publikacija4ZZPL/4PublikacijaZZPL.pdf

https://www.poverenik.rs/sr-yu/za%C5%A1tita-podataka/s-prava-zp.html

https://www.juznevesti.com/Drushtvo/Podneta-krivicna-prijava-zbog-objavljivanja-iskaza-Malcanskog-berberina-u-tabloidima.sr.html

https://www.dw.com/hr/eu-upozorio-srbiju-zbog-cenzure-na-internetu/a-17681364

https://www.cenzolovka.rs/tag/dragana-rakic/

https://freedomhouse.org/country/serbia/freedom-world/2019

https:/www.dw.com/hr/eu-upozorio-srbiju-zbog-cenzure-na-internetu/a-17681364

https://nova.rs/drustvo/kc-vojvodine-pred-pucanjem-bez-zastite-za-medicinske-sestre/

ELSA Spain

Contributors

National Coordinator

Iván Gil Puente

National Academic Coordinator

Lorena Enciu

National Researchers

Marta Beranda Menayo

Miguel Cano Menor

Alexandra Dopazo

Maria Llorente

Mario Rodriguez Barrios

Marina Rubio Alberca

Jin-Syuan Wong

National Linguistic Editor

Demian Gonzalez

National Academic Supervisor

Laura Teresa Gómez Urquijo

Roman Intxaurta

Acknowledgements

Special thank you for Roman Intxaurtieta and Laura Teresa Gomez Urquijo, for their dedication, passion and guidance.

Introduction

On the Catalonian autonomous government building, the textile fabric of the protest slogan of 'Article 19 of Universal Declaration of Human Rights: Freedom of Expression' has been changed since the outbreak of the 2017 Catalonian Independence Manifestation. Indeed, Freedom of Expression and its limitations has been one of the most contested issues in contemporary discourse in Spain, especially in the context of the ever-growing demands of Catalonian independence. The paradoxical relation between internet censorship and Freedom of Expression, in other words, the paternalistic guardianship approach of surveillance and the fostering of free thoughts and their voluntary exchange based on trust and good faith respectively lies in the fundamental value of Freedom of Expression for liberal democratic societies. After the transition from Franco's Fascist dictatorship to democracy in 1978, Spain has strived to establish itself as one on the liberal camp, both by the principles in and application of its national jurisdiction, and compliance with EU regulations, international and global legal regimes, as entrenched in Section 10.2 of the Constitution

Article 19 of Universal Declaration of Human Rights (UDHR) guarantees that 'everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers,' not only protecting the freedom of opinion and expression in the physical world but also the virtual world; meanwhile, any interference, including internet censorship, poses threats to the rights guaranteed. More sophisticated than Article 19 of UDHR, Article 10 on Freedom of Expression of European Convention on Human Rights (ECHR) also establishes a foundation such that 'everyone has the right to Freedom of Expression include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers', in conformity with Article 19 of UDHR's overarching protection of Freedom of Expression, and condemns governmental interference. However the second paragraph states that 'the exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and

are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary,' putting considerable legal and judicial constraints on Freedom of Expression for the public good, from which one can infer that the Freedom of Expression is not unconditional nor absolute, but is relational and flexible, and therefore its limitation could be subject to abuse. To avoid such unintended consequences, the balance between safeguarding the rights and Freedom of Expression, and surveilling the abusive use of such rights for harm to the society is a delicate yet significant collective endeavour of both the individual and the institutional. This report will assess such balance in the Spanish legislation.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

The most symbolic and fundamental protection of the Freedom of Expression under Spanish jurisdiction lies in Section 20 of the Constitution, whose first part has outlined 'a) the right to freely express and spread thoughts, ideas and opinions through words, in writing or by any other means of reproduction; b) the right to literary, artistic, scientific and technical production and creation; c) the right to academic freedom; and d) the right to freely communicate or receive truthful information by any means of dissemination whatsoever,' and that in the exercise of the listed freedoms, the law shall regulate the rights of personal conscience and professional secrecy. The second part of Section 20 of the Constitution has even furthered the institutional guarantee of Freedom of Expression to the extent that 'the exercise of these rights may not be restricted by any form of prior censorship,' considerably limits the possibility of state surveillance and censorship in the cyberspace. The third paragraph of Section 20 of the Constitution complicates the protection of free expression and the fostering of multiculturalism in relation to state control by stating that 'the law shall regulate the organisation and parliamentary control of the mass communication media under the control of the State or any public agency and shall guarantee access to such media by the significant social and political groups, respecting the pluralism of society and of the various languages of Spain.' Contrary to the first two clauses which are strongly in favour of Freedom of Expression, the third clause is rather ambiguous in that, while it demands legal

framework to regulate state control over media and calls for respect for multiculturalism, it also implicitly recognises the state surveillance and supervision over means of mass communication. The fourth paragraph further constrains the Freedom of Expression 'by respect for the rights recognised in this Part, by the legal provisions implementing it, and especially by the right to honour, to privacy, to the own image and to the protection of youth and childhood.' The last paragraph authorises the state to confiscate the censored publication, recordings, and other means of information, however this could only be implemented 'by means of a court order.' Despite being the most fundamental constitutional safeguard of Freedom of Expression, in defining the rights to be protected, and the limitation of such protection, Section 20 of the Constitution opens the door of diversity in legislative adoption and juridical interpretation. The relational nature of the Freedom of Expression is not only expressed by its possible limitation, but also its functional enlargement, as exemplified by Section 71 of the Constitution, 'members of Congress and Senators shall enjoy Freedom of Speech for opinions expressed in the exercise of their functions,' and the Recital of Motives of the Criminal Code of Spain (1995), 'Freedom of Expression is granted the full relevance it may and must be recognised under a democratic regime.'

Article 498 of the Criminal Code even stipulates that those who use force or intimidation of preventing a member of the Congress of Deputies, the Senate or of a Legislative Assembly of an Autonomous Community from attending its meetings, or by the same means limits free expression of his opinions or casting a his vote, shall be punished with a sentence of imprisonment of three to five years, granting special protection of the Freedom of Expression for the public function of parliamentary debate, discussion and decision making.

This functional enlargement has conditioned the definition of censorship that has been granted. Although censorship is defined as 'the suppression of speech, public communication or other information on the basis that such information is regarded as harmful or sensitive', section 20 of the current Spanish Constitution states the following: 'The exercise of these rights may not be restricted by any form of prior censorship', indicating that no form of censorship shall restrict the exercise of these rights. Nevertheless, the seizure of publications, recordings and other means of information can only be carried out with a search warrant (preferable option).

The prohibition of censorship is, since the entry into force of the Spanish Constitution of 1978, an absolute prohibition and thus does not admit any exception based on other legal prerogatives contained in the Constitution. It is,

therefore, essential to discern among all restrictions on Freedom of Expression those that can be deemed as censorship.

The concept of censorship has been provided by the Constitutional Court Ruling of the 25th of October, 187/1999, where it defined censorship as 'any restrictive measure of the elaboration or dissemination of a work consistent on a prior exam carried out by a public authority of its content, and whose intent is the seeking to judgment of the work in question on the basis of values that are abstract and restrictive of other liberties, in such a way that the publication of the work is subject of the authorisation of such authority.' Consequently, only those works that accommodate or suit the abstract and restrictive requirements will be published, refusing its publication if the work does not comply with such criteria. By virtue of this definition, only restrictions carried out by the state can be regarded as censorship, being the State the sole censor. The attacks against Freedom of Expression or Freedom of Information exercised by individuals or private parties are not deemed as censorship, but rather as simple violations of those fundamental rights, which have separate legal consequences. Freedom of Information holds a special place in our legal system, given that 'not only an individual interest is protected, but also its responsibility entails the acknowledgement and guarantee of the possibility of the existence of a free public opinion, which is indissolubly linked to the political pluralism of the democratic State itself' (Constitutional Court Ruling of the 23th of June 68/2008, FJ 3). It has been the Constitutional Court that has delimited the concept of Freedom of Information in our national legal system. However, such special protection is subject to certain immanent and external limits that this Court has progressively been outlining. Among the immanent limits are the requirements of truthfulness and of general interest or public significance of the information (Ruling of the Constitutional Court Ruling of the 1st of June, 129/2009, FJ 2; and Ruling 68/2008, FJ 3); in absence of the aforementioned requirements, the constitutional support of Freedom of Information diminishes. In light of those two restrictions, even if this right is not to be restricted to information specialists, as this right is applicable to every legal person, the juridical understanding of our legal order stems from the assumption that the subject who exercises this liberty is an information specialist. The aristocratic influence is apparent in the content of this right that courts endorse based on national case law. Not all information is protected by Freedom of Information; solely the information that is truthful and noticeable, i.e., relevant for the public opinion. That is why, in practice, the information protected by this right will be information worthy of the attention of information professionals. The requirement of truthfulness equally demands diligent elaboration and the

contrasting of information in accordance with the standards of such profession.[1893]

In order to guarantee the Freedom of Information inherent to the exercise of the aforementioned profession, the Organic Law 2/1997 regulates the so-called rights of conscience of journalists. Article 1 of this Act defines a conscience clause as the constitutional Right of Information professionals that is aimed at guaranteeing independence in the development of their profession. To pertain within the material scope of the Organic Law 2/1997, the subject must be an information professional, which ultimately refers to those professionals who are contractually linked to a media company and carry out journalistic functions within it. By virtue of the conscience clause, any information professional has the right to unilaterally rescind the contract with the company with which he takes part in journalistic functions in the following two cases:

— If there has been a substantial change in the orientation or ideology of the company with which he is contractually linked.
— If the company transfers the information professional to another legal person of the same group that has a different ideological line to that of the prior legal person where the journalist was providing its services, thus implying a breach with the professional orientation of the professional.

This right constitutes a guarantee for journalists against so-called 'internal censorship', which is the control of contents that can be exercised by the company. The functioning of mass media groups acquires remarkable importance in safeguarding Freedom of Information. For that reason, several mechanisms, including cross-media rules, have been imposed in order to limit the control of multimedia conglomerates. These rules establish a limitation to freedom of enterprise and mainly aim to guarantee pluralism of information.

The main difference between Freedom of Expression and Freedom of Information lies on the objects protected. While Freedom of Expression protects the freedom of individuals to externalise ideas, thoughts, opinions or value judgement, Freedom of Information protects the manifestation of truthful and noticeable facts. This difference entails different legal consequences, Freedom of Information does not require any veracity or truthfulness of information. Consequently, an opinion lacking a logical foundation will be as equally protected as a well-reasoned opinion. Freedom of Information is not an absolute right and, thus, it encounters limitations. In this regard, there are certain

[1893] Emilio Guichot, Law of Communication. (Iustel Fifth Edition. 2018).

contents which are not included in this right. These contents include information classified by the Central Government as 'official secrets which are regulated under the Official Secrets Act'. According to Article 4 of such Act, central governments can classify issues, documents, information, data, and objects which, in case of being known by non-authorised persons, can damage or put the security of the state at risk, as 'reserved' or 'secret'. Accordingly, access is restricted to certain content when that limitation is necessary for national security purposes. On these grounds, the protection of public order and national security prevails over Freedom of Information. Another partial limitation to Freedom of Information is the secrecy in summary proceedings. Article 120 establishes the publicity of judicial actions as a fundamental principle in every legal proceeding but allows for exceptions through the access to justice legislation. Authorised by this principle, the Criminal Procedure Act establishes in Article 301 that 'the summary records will be secret until the oral phase of the legal proceedings have not been opened'. The purpose of this provision is to safeguard both the proper investigation of the crimes and the presumption of innocence of the defendant. However, the secrecy in summary proceedings has been interpreted in unison with Freedom of Information, as any issue that is being dealt with in a criminal proceeding possesses public interest. The secrecy in summary proceedings does not exclude the possibility of journal investigations through other methods and informs over the same matter that is being investigated in the summary proceedings. The Constitutional Court has expressed in its Ruling of 15th of April, 54/2004 that as long as a journalist demonstrates the veracity and public relevance of certain information, despite it being object of judicial secrecy, the Freedom of Information of that journalist will be protected and will receive preferential protection when it clashes with other rights.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

In terms of the blocking and takedown of internet content in our national legislation the Royal-Decree Law 14/2019, which entered into force on the 6 November 2019 is essential. This specific regulation includes reasons through which the Government can temporarily withdraw physical and electrical access to access that derive to the use of the internet in a specific territorial area. This possibility is not only foreseen in this regulation but also in the Telecommunications Acts adopted in 2014. Thus, the rules on this topic cannot be found on a single body of law but they are scattered over various acts.

The mandate that is set out in the said Royal Decree does not consist of a withdrawal of the content of a website but rather it is the access in any case that is prevented from a certain moment. Thus, this decree has enlarged the range of situations to those that were already available since 2014. This possibility was already mentioned in the telecommunications law, although there were not enough legal tools that could be used for the cases, something that would be done through this decree.

What is going to be available is the access, the correct use and the use of the infrastructures that offer this support and internet access in all the areas where you can have access in Spain. The clearest example is the closing of the system of antenna network transmission systems, which would cause the internet to be inaccessible.

Articles 6 and 7 of this royal decree must be studied more in depth in order for the government to have direct management control, exceptionally in matters that undermine public order, national security and public security, thus affecting infrastructures, other resources, services and other elements.

It seems interesting to examine that, at this time, even public administrations can, not without a prior report from the National Commission on Competitions and Markets (NCCM), be controlled by the state in case of not fulfilling its obligations with citizens, although such authorities must have competence in security matters regarding the provision of public services and must prove the existence of an abnormal functioning of a telecommunications service.

In addition, the following is established 'Prior to the start of the sanctioning procedure, it may be ordered:[1894]

a) When there is an immediate and serious threat to public order, public security or national security.

b) When there is an immediate and serious threat to public health.

c) When the alleged infringing activity may cause serious damage to the operation of public security, civil protection and emergency services.

d) When other electronic communications services or networks are seriously interfered with.

e) When it creates serious economic or operational problems to other providers or users of electronic communications networks or services or other users of the radio spectrum.'

[1894] Article 6 of Spanish Royal Decree Law 14/2019.

In these sections in particular, it is in theory the administration itself that determines the moment when there is an immediate and serious threat against public order or security, national security, etc.

An in-depth study is therefore necessary to be able to perform a procedure of such magnitude as this, being possible in theory, although we will always find the pertinent doubts about when a situation is and is not intended by this procedure, when it is pertinent to act and when not. In order to execute such a procedure, it is indispensable to conduct previous investigations in a short time frame which, although theoretically possible, will always encounter doubts regarding the appropriate application of the proceedings.

For these reasons, it is understood that the adopted measures are pertinent. But there is still a lack of enough legal and research bodies to analyse the complex nature regarding the application of current legislatures concerning online activities and the situations where the NCCM must be informed. Although governmental interference in specific cases might be necessary in the future, presently such assertion is premature.

Therefore, there is not a specific legal framework aimed at the blocking, filtering or takedown of illegal internet content. This means that there are currently no legislative or other regulatory systems put in place that define the conditions and procedures to be carried out in a single body of law. Rather, they are fragmented over various areas of law. Spain relies on the existing 'general' legal framework that is not specific to the internet to conduct.

In light of the above, only two legislative acts regarding the subject-matter can be found to date: the Telecommunications Act and the royal decree that has been published a few months ago. As a consequence, there are insufficient cases to date at the Spanish jurisprudence to justly respond to individual demands in courts, since there was no normative basis to be able to correctly argue the demands of individuals or of different parties in different courts of multiple instances. Consequently, parties could not make assumptions for matters like this, obliging them to turn to the European legislation to solve the conflicts in question. Cases of censorship can be observed on the Internet in Europe with European legislation, but cases of censorship on the Internet in Spain such as the removal of the content we have not been able to find in broad strokes, since the regulations have been recent with the telecommunications law and the royal decree that completes it. This lack of regulation on the topic is the main reason for the adoption of this current legislation.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

Spanish legislation regulates the blocking, filtering, and removal of illegal content in the internet through special legislative measures which can be found in different legislations divisible into two bodies of law.

3.1 Criminal Law

Nowadays, a false sense of security conveyed to computer users has contributed to the proliferation of illegal content on the Internet. For this reason, the possibility to commit crimes through the internet is observed by the Spanish Criminal Code, regarding measures of blocking and removal of this illegal content.

Firstly, it punishes and blocks websites which contain or disseminate child pornography or use the information of disabled persons, according to its Article 189 (8). Secondly, according to Article 270 (3), when works protected by Intellectual Property rights (hereinafter, IPR) are published on the Internet without the proprietor's consent, the judge shall remove the content. Thirdly, it is established in Article 510 (6) that a judge will order the removal of content inciting hatred and when the content of a website or a service of information society is of predominantly hate-inciting nature, it will be blocked or interrupted.

Nevertheless, the causes for removing internet content are not only set out in the Criminal Code but also in the Information Society Services and Electronic Commerce Act. According to Article 8, there are a series of principles which justify blocking and taking down content, such as terrorism and sexual abuse.

The procedure assigned to these cases is the following: in case a determined hosting service provider detects a breach in said principles, the responsible bodies are enabled to take action and adopt the necessary measures to block or take down the content[1895]. Once they have judicial authorisation, they are legitimated to require the information society services to facilitate the necessary information to identify the breaching user. The information society services have the legal obligation to collaborate, as stated in the Royal Decree 424/2005 in Articles 61.3, 83, 93 and 97. Though it is the individual who must identify the breaching content and prove why it should be taken down, the hosting service

[1895] Javier Álvarez Hernando, 'Material and procedural aspects of illegal content take down on the Internet' (AC Abogados, 8 June 2011), <https://bit.ly/2UF1tQu> accessed 07 February 2020.

provider has subsidiary responsibility in case the content is not taken down or blocked after notice[1896].

It is important at this point to mention Article 13 of the Criminal Procedure Act (Spanish procedural law). This Article gives judges the capacity to adopt provisional measures in order to examine all criminal evidence and verify the offender. These measures can nevertheless become definite if needed. If the accusation is made by an individual instead of state authorities, it is important to provide a copy of the content in order to facilitate further judicial proceedings. Up to this point in the procedure, the offender does not intervene regarding the taking down or blocking of the content. It is the judge's role to evaluate whether any rights and liberties (particularly regarding Freedom of Expression) could be endangered in the situation to subpoena the parties involved for a hearing. In both cases, the judge must act proportionately and provide proof in the judicial decree, which must be resolved within a maximum period of two days.

In Spain, judges aren't the only competent authority regarding this kind of restrictions on the internet. There are other administrative authorities such as the Intellectual Property Commission, further explained below, or the Spanish Agency for Data Protection, which have certain mechanisms in place to block and take down determined kinds of content. The Spanish Agency for Data Protection has a so-called 'priority channel' in which an individual can denounce the trafficking of pictures and videos of sexual content or aggressions, where the rights and liberties of the affected may be at risk. This plays an especially important role in cases concerning minors or gender-based violence victims.

3.2 Civil Law

The owner of IPR who detects an infringement of his rights may apply for an injunction to restrain the unlawful activity following the Articles 138 and 139 of the Intellectual Property Act (hereinafter, LPI). More specifically, the right holder is entitled to request the removal of the works containing its IPR from the internet.

In order to ensure the protection of IPR online, the intermediary service providers (hereinafter, ISP) must take down the content declared illegal or unlawful by a judge or a court, according to Article 11 of the Information Society Services and Electronic Commerce Act (hereinafter, LSSI). Following this legislation, these measures are justified regarding the protection of national security, public order, and national defence, the safeguarding of public health,

[1896] Carolina Pina and Cristina Mesa, 'EU Recommendations on take down of Internet content' (Garrigues Digital, 23 March 2018), <https://bit.ly/377XrlX> accessed 06 February 2020.

the respect for personal dignity, the principle of non-discrimination, and the protection of the reputation of rights of others (Article 8).

These restrictions to Freedom of Expression must be objective, proportional, and non-discriminatory, and they will be adopted as a precautionary measure or in execution of a resolution issued, in accordance with the established administrative procedure or those provided for in the procedural legislation.

The competent judicial authority, as guarantor of the right to Freedom of Expression, may exclusively adopt these measures as protective measures when the requirements are fulfilled (Articles 721 *et seq* of the of Civil Procedure Code), which can be requested in a civil claim or even before if the civil claim is filed within the term of 20 days after the request of protective measures. However, the blocking or removal of illegal or unlawful content is usually adopted in a civil or criminal judgment.

But in Spain there is also an Intellectual Property Mediation and Arbitration Commission created by the Ministry of Culture. Among its competences, section 2 states that it is responsible for safeguarding IP rights in the digital environment in accordance with Article 195 of the LPI. Therefore, it is entitled to adopt measures to interrupt these unlawful conducts on the internet, requiring the ISP to cease the infringement.

The procedure is the following: firstly, when an infringement is observed, the owner of IPR or the collective management organisation must request the information society provider to remove any unlawful content on the internet within a three-day time frame. If it is unsuccessful, he may address this Commission.

Secondly, the Commission will demand the information society service provider to voluntarily withdraw the contents within a term of not more than 48 hours or to submit the pleading and propose the evidence regarding the authorisation for the use or the applicability of limits to the IPR. The conclusions shall be notified to the parties involved within five days and the Commission shall hand down a decision within three days. The decision handed down by this Commission shall put an end to administrative channels and it is appealable to the Administrative Jurisdiction.

As it can be observed, Spanish procedural law has fixed considerably short deadlines for the present procedure, indicating a sense of urgency. This is because of the possible infringement of fundamental rights, such as those in Article 20 of the Spanish Constitution. For this, it is believed that the mechanisms in place are sufficient and effective, as are the ways in which a

citizen can effectively exercise inherent rights (judicial, administrative, arbitrative) and, therefore, the degree of legal protection increases.

According to the Supreme Court, new technologies intensify the damage of affirmations or messages which, at another time, could have limited their harmful effects to a small and selected group exponentially[1897]. This assertion is disproportionate because, even if messages on the internet can potentially affect many individuals, only a specific analysis of each case allows us to conclude if it reached remarkable diffusion[1898]. As a result, it denotes a fearful approach to the digital era.

Criminal courts have ordered the removal of content on the internet because the such exhibitions constitute a criminal offense for glorifying terrorism. Some tweets were considered to incite violence, as they praise terrorist groups, and they were also published for an extended period of time[1899]. Moreover, songs published on social media have been taken down for similar reasons[1900], particularly for inciting terrorism, as they mentioned and glorified terrorist groups in their lyrics.

In other situation[1901], tweets and songs were removed for being considered humiliating to terrorism victims and their families because they glorified and justified terrorist crimes committed in Spain. They are removed because they collide with the expression of solidarity with the prisoners or political support, the violent means used, and the repetition of the comments which are not protected by the Freedom of Expression. Likewise, there were expressions which exceeded political criticism, attacking on the reputation and honourability of the King of Spain and charging him with inexistent crimes. Also, they contained insults or serious threats to the Spanish Army and National Security Forces.

Likewise, the Civil and Commercial Courts can also block websites when they infringe Intellectual Property Rights. The Commercial Court of Barcelona partially blocked a website because it presented exact copies of Adidas products[1902], using its registered trademarks and designs. The IP Commission

---

1897 Judgement of Supreme Court No. 4/2017 of January 18th, 2017.

1898 TERUEL LOZANO, G.M, "Expresiones intolerantes, delitos de odio y libertad de expresión: un difícil equilibrio", Revista Jurídica Universidad Autónoma de Madrid, No. 36, 2017-II, page 194.

1899 Judgement of the High National Court (Criminal Chamber, Section 1) No. 4/2018 of July 10th, 2018

1900 Judgement of the High National Court (Criminal Chamber, Section 1) No. 6/2018 of the 18th of September, 2018.

1901 Judgement of the High National Court (Criminal Chamber, Section 1) No. 3/2018 of the 2nd of March, 2018.

1902 Order of the Commercial Court of Barcelona, No. 195/12 of the 30th of April, 2012.

has also ordered the removal of a song by Spanish singer Luz Casal from a website for having been uploaded without authorisation[1903].

Censoring is defined as 'any measure restricting the product of the human intellect, in particular by making it dependent on prior official examination of its content'[1904]. Firstly, in order to guarantee this right, prior censure is forbidden in Article 20 (2) of the Spanish Constitution. Secondly, the content which must be censored is determined by the aforementioned Criminal and Civil Law. Thirdly, these measures are taken by competent judicial authorities following an established procedure where they analyse the protection of other rights that could be harmed by the dissemination of such illegal and unlawful content.[1905] Consequently, a balance exists between censorship and Freedom of Expression as the diffusion of content on the internet is only removed when it affects fundamental rights of others.

Following this reasoning, compliance of the Spanish regulation with the ECHR and the related case law should also be evaluated. Imposing the so-called 'triple test' through the Article 10 (2) of European Convention, reduces the possibility of interference with the Freedom of Expression[1906]; they must meet the following criteria: be prescribed by law which is accessible, clear, unambiguous, and sufficiently precise to enable individuals to regulate their conduct, have a legitimate and proportional aim, and must be necessary in a democratic society.

The Spanish Constitution requires in Article 20 (5) that only the judicial authority is competent to take measures which can restrict Freedom of Expression. Therefore, it is the only competent judicial authority, as guarantor of this right, that can authorise the implementation of measures considered by the second section of IP Commission.

Following Article 8 (1) LSSI, when measures are taken to block or remove content on the Internet, the guarantees, norms, and procedures provided for by law in order to protect Freedom of Expression where it may be affected must be respected in all circumstances. Likewise, when Article 11 (3) and (4) of the same legislation refers to the obligations of the ISP to cooperate, it also demands respecting and guaranteeing Freedom of Expression and requires the ISP to take

[1903] Case No. E/2012/00012 of the IP Commission.

[1904] STC 52/1983, de 17 de junio, FJ. 4.º y en términos similares STC 13/1985, de 31 de enero.

[1905] TERUEL LOZANO, G.M, "Libertad de expresión y censura en internet", Estudios de Deusto, Vol. 62/2, Bilbao, Julio-Diciembre 2014, pages 60-61.

[1906] Voorhoof, Dirk. (2015). The European Convention on Human Rights: The Right to Freedom of Expression and Information restricted by Duties and Responsibilities in a Democratic Society. Ḥuqūq-i Bashar. 7. Page 6.

objective, proportional, and non-discriminatory measures following the established procedures.

To this extent, it can be claimed that Spanish Laws meet the requirements of the ECHR, firstly because the list of motives for filtering, blocking, or removing content on the internet is limited and secondly because only the maximum judicial authority can request these measures.[1907]

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

Article 1255 of the Civil Code sets out the principle of party autonomy. Nevertheless, the contractual freedom finds it limits in the imperative legal provisions and the legal consequences of the contract and thus requires the positive intervention of the State in order to sanction the non-compliance of the national legal order and of the stipulations by the parties.

Article 18 of the Information Society Services Act regulates the Codes of Conduct. The elaboration of these private documents is voluntary and parties are able self-regulate the procedure to detect and block illicit content through it. This rule thus habilitates private parties to set the criteria and principles for the removal of content online.[1908] Regarding the private sector, no express regulation for the takedown and blocking of internet content can be found in the Spanish legal order, remaining to the party autonomy of the internet service providers. Consequently, self-regulation has been adopted by the private sector to supplement the void left by the legislator's choice not to intervene in the area at stake at a private sector level.

4.1. Safeguards to protect freedom of expression online

The safeguards in place for ensuring the protection of freedom of expression online where self-regulation is applied are the following:

The Spanish legislation has sought to find a balance between guaranteeing the parties' autonomy while protecting the interests of vulnerable groups. For this purpose, it has been set out in paragraph 2 of the aforesaid provision a mandate on the protection of weaker parties in the contract. When the content of these Codes of Conduct affects the interests of both consumers and users as well as mentally and physically disabled individuals, the Codes of Conduct should take

[1907] ARONOVITZ, A., "Comparative study on blocking, filtering and take-down of illegal Internet content", Swiss Institute of Comparative Law, Avis 14-067, 20 December 2015, pages 641-664.
[1908] Boletin Oficial del Estado. Information Society Services and E-Commerce Act.

due regard to these interests, being necessary, at times, that specific codes on these matters are elaborated. This provision guarantees that these interests are taken due regard to the participation of consumer associations and organisations that represent disables persons, which is fixed as a prerequisite for the adoption of Codes of Conduct when they affect any of those two groups. By requiring the participation of these actors in the negotiations, it is guaranteed that these documents are not adopted unilaterally, but rather as a *trait d'union* or a nexus of the interests of these 2 groups.[1909]

In paragraph 3 of this provision, it is laid down that these Codes of Conduct are to be accessible via the internet. Therefore, its publicity through electronic means is a requirement for its validity, not being licit if the Codes are kept secret.

It is also essential to mention the action of Public Authorities regarding these methods of self-regulation. They essentially play a role of promotion, by imposing these codes through the coordination and the counsel of their elaboration. However, the way this function is exercised is not further developed, thus, it is left to the discretion of each Administration its inclusion among its functions.

In the field of self-regulation an essential guarantee is that which is granted by Data Protection rights. The Right to the Protection of Personal Data guarantees, on the one hand, that citizens can participate in conditions of freedom in society and, consequently, in , the formation of a free public opinion; on the other hand, as the Spanish Constitutional Court has concluded, with the recognition of Freedom of Expression and the remaining rights of Article 20.1 of the Spanish Constitution, it is also guaranteed: 'the maintenance of a free public communication', without which other rights that the Constitution establishes and distorted the principle of democratic representation outlined in Article 1.2 of the Constitution, and which is the basis of all our legal-political ordering, would be emptied of real content. then, the right to data protection takes on an instrumental nature of the guarantee, since it guarantees freedom of action, since the possibility of acting freely 'in private' conditions our free performance 'in public'.

Therefore, since the Right to the Protection of Personal Data is a guarantee of the exercise of Freedom of Expression and information, this right also becomes a guarantee of the formation of free public opinion. We must remember that this is the ultimate basis of the Right to the Protection of Personal Data, so, in addition to the above mentioned, if the person is deprived of that right, he or

[1909] Lopez, David. New Coordinates for the Law of Contracts. Self-regulation in E-commerce. 2013.

she is being deprived of his or her development; , thus limiting the possibility of what the citizen can enjoy the rest of fundamental rights, among which we find Freedom of Expression and information, ultimately damaging the democratic principle. If individuals are aware of data related to their person that is known by other citizens or public authorities, they may participate more freely in the democratic society and thus create a free public opinion, necessary for the proper functioning of a Social State and democratic law.

As a result, the protection of personal data becomes a guarantee of freedom of action and thus of Freedom of Expression and information, essential elements of a Social and Democratic *État de Droit*. In this way, the democratic principle will be realised by guaranteeing that all individuals can participate in the political decision-making process based on the principles of freedom and equality.

In Spanish legislation, an arbitration procedure is foreseen in Article 32 of Law 34/2002. This Article leaves the service provider and user the option to resort to an extrajudicial procedure. As a consequence, all these safeguards are to be exercised in an arbitration procedure or in a court of law.

In light of the above, self-regulated notice and take down procedures that are in place, do not offer sufficient guarantees, especially from the due process perspective. In this context, it has been argued that states do not merely have a duty not to interfere, but must protect fundamental freedoms, and this especially in relation to access providers. Nevertheless, when it comes to codes of conduct through which these procedures are regulated, the role of the State is constrained to a promotional role, not being specified the way this intervention is carried out.

Nevertheless, there are also benefits for the usage of this method of self-regulation, for instance if a company has a code of conduct that has a probationary value regarding the obligation of information they must fulfil. Moreover, Codes of Conduct play an essential role of accommodating the needs of the technological sector, and e-commerce in particular, to the national legislation. In terms of its affection in the organisation of the firm, Codes of Conduct establish behavioural norms, binding all the adherents. These norms specify reprehensible conducts that will receive the sanction of blocking or taking down content as a result of breaching the ethical standards of that firm. They can also serve to provide quality to the services or goods of the company. Despite this, the underlying motivations for the elaboration of these codes of conduct are at times mainly related to the image or reputation of the image. They can be elaborated with the main purpose of creating an image of trust and reliability to consumers. As a consequence, it is important that our national

legislator sets up mechanisms to safeguard the correct application of these codes and to protect public interests that might be left unattended due to private application.

4.2. Models in place

When it comes to these codes of conduct, which is the main method of self-regulation that is utilised for the removal or restriction of access of a content in the Spanish legal order, different models can be found. By reasons of the recipients of these codes of conduct, they can be either codes of conduct addressed to customers or users and those that are addressed to corporations. The latter refer to those codes of conduct that are applied in the commercial relationships or legal relationships between different corporations, thus being codes that are merely B2B. The former, involve codes created for the legal relationships with the consumer, who becomes the weaker party. That is why the Spanish legislator has provided for the safeguards explained above, especially the involvement of associations of consumers in the elaboration of these codes. These B2C codes can regulate interactive publicity and e-commerce matters in a generic way or they can be created for the provision of specific services, such as blogs, virtual games, wikis, medical services, etc.[1910]

4.3. Assessment of grievance redressal mechanism

It is commonly believed that the Spanish legal system is rather a guarantee-based system in comparison to others. This makes it easier for the population in case they must appeal the decision, given that they have an appeal system which provides for a process in which the parties can and must be heard. In the private sector regulations, intellectual property breaches account for many of the systems in place. In this concrete matter, and regarding the Intellectual Property Commission, the breaching user will be required to take down the content himself in less than 48 hours as it has been explained before.

Social networks are of great significance when talking about blocking and taking down content. One of the main reasons why this happens is because of copyright infringement, but there are many other reasons. In order to block or take down content in these information society services it is not necessary for the content to be illegal; it is enough that it is considered as harmful or inadmissible content to be taken down. Each service's terms of use define these concepts, allowing them to adapt this kind of measures to the particular business[1911]. In relation to

[1910] Lopez, David. New Coordinates for the Law of Contracts. Self-regulation in E-commerce. 2013.

[1911] Pedro Alberto de Miguel Asensio, 'Take down and blocking of Internet content: Commission Recommendation implications' (Pedro Miguel Asensio, 7 April 2018), <https://bit.ly/2uA4KWi> accessed 05 February 2020.

big enterprises like Instagram or YouTube, they each have a concrete mechanism through which they address this matter. YouTube guides itself through what is called Content ID, which identifies material which colludes with already uploaded original content and notifies the affected user. This gives the users the option to choose if they want the video to be taken down or only to readdress its profits to their own benefit.

In many cases, the social network mechanisms are quite similar in every country. According to points 18, 19 and 20 of the Commission Recommendation 2018/334, hosting service providers are allowed to use a series of proactive measures in respect to illegal measures but have to take into account the safeguards in the next two points. In Spain, in case a person detects a breach of any regulation regarding personal data, it is possible to fulfil an incident report at the Spanish Agency for Data Protection. This will allow the user to protect her/his rights, as well as have a quick answer to the conflict.

4.4 Inconveniences of self-regulation

Voluntary suppression of information by private actors comes with various drawbacks. The decisions of privately owned platforms and internet service providers are sometimes triggered by direct political pressure or from politically motivated economic compulsion, invoking the terms of conditions as the basis of the action of blocking or taking down content. The engaged companies are not immune to undue interference. The Council of Europe Commissioner for Human Rights expressed in 2014 the serious doubts on whether the self-regulating blocking system will be in accordance with the rule of law. The imposition of restrictions on the access to online information is carried out by private parties, with a total absence of private parties and public scrutiny.

5. Does your country apply specific legislation on the 'right to be forgotten' or the 'right to delete'?

For some the right to be forgotten originates from the endeavours of the Commission Nationale de L'informatique et les libertés, while for others it seems from the ruling *Melving v. Reid* of the California Appellate Court. Nevertheless, the legal requirement for the deletion of harmful content is not a new figure in the Spanish legal order. Prior to the introduction of the Right to be Forgotten into our national legislation, we find institutions such as the cancelation of the criminal record or the anonymisation of legal rulings before they are to be

published, whose aim is to safeguard the private sphere of the individual, the free development of one's personality and insertion in society.[1912]

Data management and processing are omnipresent in the information society of the digital age. The automatic and distance-less data sharing and proxy data management of the digital age not only makes its employment stand out from the traditional data management, but expose it to risks of exploitation, right infringement, and harm.

On the European level, the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018 are the first line of defence against infringement on individual property and privacy with unfair and unreasonable data processing, among other means. However, this is only the first European legal attempt to confront the war on information, as there still remains enormous concerns of violation of data privacy.

Originally designed in 1990s, those data protection frameworks were constructed for the traditional data manipulation with storage and processing on computers, which has been outdated in the digital age where data collection and diffusion take place ubiquitously, automatically, and instantly, sometimes even without data property owner knowing it, in the proxy form of data management. Therefore, the frameworks protect data integrity and security rather than specifically data privacy. (Murray 2019:617-618)

The Right to be Forgotten (RTBF), according to the definition given by Article 17 of GDPR on Right to Erasure, refers to 'the [data subject's] right to obtain from the controller the erasure of personal data concerning him or her without due delay' when grounds of application are met. The salience of RTBF entrenched in international and national legal frameworks was established in the aftermath of the ground-breaking case of Google Spain SL and Google Inc. v AEPD (ECLI: EU: C: 2014: 317).

In the late 1990s, a Spanish citizen, Mario Costeja González, was the data subject of an announcement on the newspaper La Vanguardia for the purpose of public auction of real estate property, as he owed the Spanish Ministry of Labour and Social

Affairs debts by means of social security payments. Following the extinguishment of debt, La Vanguardia digitalised the newspaper with content information on the public auction of Mario Costeja González's property, and this information was later indexed by Google, meaning that it could be found in the searching results if his name is the keyword. According to Article 6(1)(c) of

[1912] Ana Isabal Berrocal Lanzarot, Right to erasure or Right to be Forgotten (Editorial Reus, 2017).

the 1995 EU Data Protection Directive, data must be 'adequate, relevant, and not excessive,' and Article 8 of the Charter of Fundamental Rights of the European Union, one has Right of Data Privacy.

With possible infringement on those legal principles, economic damage, and personal reputation suffered from this publication, Mario Costeja González filed a complaint with the Spanish Data Protection Agency, *Agencia Española de Protección de Datos* (AEPD) in 2010, as Professor Murray describes 'claiming that La Vanguardia must delete or amend the irrelevant data in a way to prevent his identification and that Google must stop linking to it in search returns' (2019: 610).Later, AEPF reasoned that as La Vanguardia simply recorded their legally published data, no actions are needed to be taken; however, they found that in producing search returns, Google is de facto processing the data, therefore subject to data protection provisions.

This case was eventually brought to The Court of Justice of the European Union (CJEU), who, after balancing between protection of data privacy and private censorship of data, found that González's claim was justified on the grounds such that 'in order to comply with the rights laid down in those provisions (Article 12(b) and 14(a) of Data Protection Directive) the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful. Therefore, it was concluded that a search engine, when it searches the web for information and web pages and when it indexes content to provide search results, becomes a data controller to which responsibilities and obligations apply. The CJEU has given the concept of 'processing data' a broad meaning, raising the threshold significantly. The condition of the data controller was substantiated on the possibility of establishing a detailed profile of an individual through search results.[1913]

The CJEU also concluded that individuals have the right to request personal data to be erased, where information relating to an individual is inaccurate, inadequate, irrelevant or excessive for the data processing purposes. Each request for erasure must be assessed on a case-by-case basis to strike a fair balance between the Right to the Protection of Personal Data and Private Life of the data subject on the one hand and the legitimate interests of all internet

[1913] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law (Publications Office of the European Union, 2018)

users, on the other. This pronouncement grants the right to users to request the definition of personal data from the search results of a search engine. Google, offers a form to fill in by the affected users, whereby the URLs that wish to be removed from the search result and the cause for that removal, must be indicated. Nevertheless, this form solely guarantees the removal of content within the territorial limits of Europe, but the data continues to appear outside of the EU territorial ambit.

In light of the above ruling, the CJEU declares the fair balance that must be sought in the erasure of content from search engines. A fair balance must be struck between the legitimate interests of internet users in access to information and the data subject's fundamental Right to the Protection of Privacy and Personal Data. Despite the balancing provision set out in the judgement, newspapers and journals at a National and European level criticised this ruling as a form of private censorship; Google also challenged this ruling by asking clarification; and UK House of Lords concluded that 'neither the 1995 Directive, not the Court's interpretation of the Directive, reflects the current state of communications service provision, where global access to detailed personal information has become part of the way of life' and that 'it is no longer reasonable or even possible for the right to privacy to allow data subjects a right to remove links to data which are accurate and lawfully available.' Despite the criticisms on the grounds of internet censorship and digital reality, from the point of view of data protection, the court ruling has given RTBF an unprecedented juridical weight.

A closer examination would even find out that the ruling of Google Spain is indeed a well-balanced approach as the RTBF only 'concerns the delisting of links from the search results, and only for searches made on the basis of the data subject's name, with the implication that no information is actually deleted.' (Peguera 2015: 329) Therefore, the Freedom of Expression is preserved to the extent that the actual publicised information is left intact except for the name listed. In fact, in many of AEPD's cases, requests of removal of information published in media outlets were rejected as the constitutionally entrenched value of Freedom of Expression and of information as public interests prevail over rights of data protection (Article 18.4 of Spanish Constitution) as long as the information remains truthful and publicly relevant. However, AEPD also advices media publishers to 'reflect about the consequences of permanently making accessible data which may no longer have any public interest, and how this could affect individuals' privacy.' (Peguera 2015: 343) As AEPD's decision of the 16 December 2014 (TD-01369-2014) shows, AEPD recommends that media publishers use technical means to avoid indexation by searching engines

'where there is a legitimate interest of a data subject and the information is no longer relevant.' (Peguera 2015: 343).

There has been a recent ruling by the Supreme Court, where the Court has declared that the data subject that has been affected by a breach to his personality right and the right to protection of private life has the legitimacy to claim the provider of the search engine services or to file an action against such provider vis-à-vis the AEPD, when the search results offer erroneous or inexact data that 'imply a devaluation of the reputational image that proves to be unjustified'. Therefore, this ruling is extending the responsibility to internet service providers of search results, who do not have the consideration of editors but nevertheless disseminate and facilitate the access to the incorrect or inexact data.[1914] This sentence is a manifestation of a jurisprudential line that states that the appearance of information in search results have a bigger affectation over the individual fundamental rights than its publication in the concrete website. The Right to Erasure should therefore be guaranteed in these cases. The Court further added that the internet service providers of search results exercise their commercial activity lawfully when they put at the disposal of the public tools of locating information of natural persons, which is protected by the Freedom of Information. Nevertheless, they are obliged to preserve to the same intensity as editors the fundamental rights of the private life of the affected data subjects, preventing any illegitimate interference in the private sphere of the individual.

Turning to the processing of data of the editors or web pages, the same balance should be struck as in the processing in search engines. In the case of El Pais, which reached the Constitutional Court, in 2007 the newspaper El Pais provided for open access to a newspaper archive of the 1980's concerning the dismantling of a drug trafficking network, the imprisonment of the convicted subjects and their addiction. This news Article included their identification by its name, surname and profession. As a result, with the introduction of the names of the applicants in the Google search engine, such news Articles appeared as the first search result. El Pais refused the erasure of this data or the substitution of the names and surnames of such individuals by its initials, on the basis of the Freedom of Information and the impossibility to avoid the indexation by the external search engines of such news Articles. The applicant asks against a court of law for the suppression of the personal data that concern the applicant from the source code of the website that contained the information, as well as urging for the prohibition of indexing such personal data for the usage by the internal search engine managed by the defendant. The Public Procurement Office was

[1914] Judgement of the Constitutional Court 12/2019, de 11 enero 2019.

favourable to the measure of deindexing the data from the internal search engine. It however regarded as disproportionate the removal of the name and surname of the applicants for the source code of the website where they were included, as it was contrary to the Freedom of Information.[1915]

The Constitutional Court in order to consider the appropriateness of removing or deindexing such data first strikes a fair balance between Freedom of Information on the one hand and the Right for the Protection of Private Life and the Right to the Protection of Personal Data on the other. So long as the data is truthful and relevant for the 'formation of public opinion', the Freedom of Information will prevail over the rights that concern the private sphere. In that event, the suitability of the erasure of data will thus prevail. In the case at issue, this prevalence of the Freedom of Information at the time of the publication in the 1980's remains unquestionable. The general interest and the public relevance of the information of events with a criminal nature constitute reiterated jurisprudence of the Constitutional Court. Nevertheless, the time frame needs to be taken into regard. As the ECtHR mentioned, the incorporation of personal information into databases implies that with the passing of time, a research function prevails over the informative functions that these data has at the time it is first included into the database.[1916]

In light of the above, the Court reached the following conclusion. The information is of public interest and complies with the requirement of veracity in terms of its content, mainly the drug trafficking and the addiction. Nevertheless, the applicants were not at the moment the facts took place exposed to public scrutiny or critique, they were not public characters, and the news lacks, after more than 30 years, of relevance for the formation of public opinion. As a result, the Court deems the erasure of the name of the applicant or their substitution into acronyms in the source code as excessive, but declares that the prohibition of indexing personal data into the internal search engine constitutes a fundamental limitation to Freedom of Information.

In terms of national data protection legislation, the new Spanish Data Protection Act (Organic Law 3/2018) on the Protection of Personal Data and the Guarantee of Digital Rights was published on the 6 December 2018, the Constitution Day, and has come into force the next day. According to Article 1 of Organic Law 3/2018, it not only harmonises the GDPR with Spanish legislation by adopting the latter in conformity with the former, but also further

[1915] Sentencia de la Sala Primera del Tribunal Constitucional 58/2018, de 4 de junio.

[1916] Right to be forgotten. Rodrigo, Bercovitz Rodríguez-Cano. Revista Doctrinal Aranzadi Civil-Mercantil num.10/2018. Editorial Aranzadi, S.A.U.

specifies several provisions of GDPR and regulates other on-going digital activities, regarding data protection and rights of information, including but not limited to right to internet access, digital education, correction on the internet and digital disconnection in the workplace, the obligation for controllers to inform its employees about the existence of the whistleblowing systems, the repurposing of personal data for research purposes and the criteria for effective pseudonymisation.

6. How does your country regulate the liability of internet intermediaries?

First, it is necessary to define what can be understood as *internet intermediaries*. The concept of internet intermediaries is defined in the Directive 31/2000/CE, the Information Society Services, and Electronic Commerce Act. The Directive classifies the intermediaries into three different groups: 'mere transaction' intermediaries in Article 12, which mainly act as a recipient source for the transfer of information or provide access to a communications network; 'catching' intermediaries in Article 13, which transmit data coming from the recipient of the service through a communication network; and 'hosting' intermediaries in Article 14, where the storage of information is provided by a recipient of the service.[1917] On the other hand, this concept is defined in the Annex of the previously mentioned Act by the Spanish legislation, in which an 'internet intermediary' is considered such if it facilitates the provision or use of other services of the information society or the access to information. Activities such as provision of internet access services, data transmission through telecommunication networks, temporary copies of internet web pages requested by users, or provision of search, access, and data collection tools or links to other internet sites, are included in this category.[1918]

In Spain, internet intermediaries are subject to civil, criminal, and administrative liability. Thus, they could be sued if they incur in any criminal activity that falls within the scope of those legal boundaries.[1919] However, there are specific provisions – Article 13 to-Article 17 – in the Information Society Services and Electronic Commerce Act regarding liabilities concerning intermediary activities. Generally, network operators and telecommunication providers´ access to

[1917] Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1 (Directive on electronic commerce).
[1918] Information Society Services and E-commerce Act 34/2002, of 11th of July, (España: Jefatura del Estado, 2002).
[1919] LSSI, Article 13.

telecommunications networks will not be liable for the information that is spread through them, unless they are the ones that have initiated the transmission of data.[1920]

Service providers that make temporary copies of the data requested by users will not be liable for the content if they take down the content when they have effective awareness that such information has been taken down from the original network place, that access to the information has been precluded, or that an administrative body has ordered it to be removed.[1921]

Service providers that host data[1922] or provide links to content or search tools[1923] will not be liable when they do not have effective awareness that the information or activity is illicit or harms rights of any third party susceptible to compensation; or, if they acted diligently when they had effective awareness of such content. Therefore, the main issue is to determine where it can be affirmed that a service provider had 'effective awareness'. This provision states that it occurs when a competent body has declared the unlawfulness of the content, ordered its removal and the service provider knew about such legal decision.

The 'effective awareness or knowledge' requirement was also established in the Directive[1924], but it permits Member States of the European Union to decide on the possibility of introducing specific requirements, such as duties of care. There is a duty of collaboration for service providers when a competent body decides to take down or stop the provision of a service[1925]. In that case, the service providers may be obliged to take down the intermediary service used to provide the service. However, even if Member States can establish a duty of collaboration or communication for service providers, it is not mandatory to monitor the data that is hosted in their services, nor actively search for circumstances that may indicate illicit activities[1926], as stated in the Directive.[1927] Hence, it can be deduced that the internet intermediaries will be subject to general Spanish rules regarding liability and, additionally, to these specific rules that are established in the LSSI, which are a transposition of the Directive on electronic commerce. Nonetheless, these provisions establish a framework for a liability exclusion.[1928] If it is proved that the actions of service providers do not fall under the scope of the liability

[1920] LSSI, Article 14.
[1921] LSSI, Article 15.
[1922] LSSI, Article 16.
[1923] LSSI, Article 17.
[1924] Directive on electronic commerce (46).
[1925] LSSI, Article 11.
[1926] Directive on electronic commerce, Article 15.
[1927] Javier Maestre Rodríguez,'The liability of information society service providers and the new concept of public' (2017) 49 Revista Derecho y Sociedad
[1928] Miguel Peguera Poch, The exclusion of liability of internet intermediaries (COMARES, 2007) 292.

exclusion, we will then have to establish which are the applicable liability rules. In this case we would be subject to non-contractual liability, which takes us to the Spanish Civil Code, more specifically to Article 1902 – civil liability of third parties – as well as to the Law for the protection of consumers and users (TR-LGDCU).[1929]

In terms of the criminal liability, by virtue of Article 30 of the Spanish Criminal Code, the liability of information society service providers is always subsidiary to that of the author of the illegal content, whose dissemination constitutes a criminal breach. Nevertheless, this precept expressly refers to mechanical means of dissemination. Due to its wording, this Article is not applicable to information society services providers and thus their responsibility will depend on their categorisation of this provider into either author or participant. Consequently, the liability of the cited provider requires personal development or cooperation regarding the unlawful content, excluding those providers that merely facilitate the service as they do not have effective awareness of the facts. Contrariwise, if the internet intermediary had effective awareness or knowledge of such content, he would be liable for the crime committed by the author.[1930]

6.1. Does an obligation to implement the measures for blocking and taking down content exist?

About restrictions to freedom to provide services, such as blocking or taking down content, the Directive states that it is not mandatory for intermediaries to control the information that is hosted in their services[1931]. However, intermediaries will be liable when they had effective awareness of illegal content hosted in their servers and they did not take down the content or block it. Additionally, the Directive leaves the establishment of obligations for intermediaries to inform public authorities of illegal activities or information hosted at their servers at the discretion of Member States.[1932] In Spain legislation there is a provision in Article 8 of the LSSI that allows competent administrations to implement measures to take down or stop the provision of content that violates certain principles :the safeguard of public order, protection of public health, consumers and users, dignity, non-discrimination, infant protection, and intellectual property safety.[1933]

[1929] Roberto Yanguas Gómez, *Internet connexion contracts, "hosting" and searches* (1st. Edn, Aranzadi, 2012) 426.
[1930] Susana Navas Navarro y Sandra Camacho Clavijo, Digital Market- Legal principles and rules (Tirant lo Blanch, 2016) 135.
[1931] Directive on electronic commerce, Article 15.
[1932] ibid.
[1933] LSSI, Article 8.

6.2 Are there any safeguards in place for ensuring the protection of freedom of expression online?

The Spanish Constitution, in Article 20, establishes the Constitutional principle of Freedom of Expression, by any means of reproduction, so it can be inferred that electronic means are regulated under this provision. There are several provisions in the LSSI where Freedom of Expression is protected, especially when adopting measures for taking down and removing content online. For example, in Article 8 of the LSSI, measures that can be taken have to respect Freedom of Expression and Freedom of Information[1934], as is reiterated in Article 11 LSSI. Nevertheless, this is a very controversial point because the Right to Freedom of Speech sometimes conflicts with other rights, such as the Right to Honour. In these cases, there must be a judicial body that declares which right prevails in each situation and, hence, impose the liability on the offender.

The issue when exercising the Right to Freedom of Speech is whether the service provider is also liable or not, when the person whose opinions or information that were hosted in their servers has been found guilty. This concept is defined in the Annex of the previously mentioned Act by the Spanish legislator, in which an 'internet intermediary' is considered such if it facilitates the provision or use of other services of the information society or the access to information. Activities such as provision of internet access services, data transmission through telecommunication networks, temporary copies of internet web pages requested by users, or provision of search, access and data collection tools or links to other internet sites, are included in this category In Spain, internet intermediaries are subject to civil, criminal and administrative liability, thus, they could be sued if they incur in any criminal activity that falls within the scope of those legal areas.[1935] However, there are specific provisions – Article 13 to Article 17 – in the Information Society Services and Electronic Commerce Act regarding intermediary activities for liability. Generally, network operators and telecommunication providers access to telecommunications networks will not be liable for the information that is spread through them, unless they are the ones that have initiated the transmission of data.[1936]

Service providers that make temporary copies of the data requested by users will not be liable for the content if they take down the content when they have effective awareness that such information has been taken down from the original

[1934] LSSI, Article 8.
[1935] Article 13. of the Information Society Services and Electronic Commerce Act.
[1936] Article 14. of the Information Society Services and Electronic Commerce Act.

network place, that the access to the information has been precluded, or that an administrative body has ordered to take it down.[1937]

Service providers that host data[1938] or provide links to content or search tools[1939] will not be liable when they do not have effective awareness that the information or activity is illicit or harms goods or rights of a third party susceptible to compensation; or, if they acted diligently when they had effective awareness of such content. Therefore, the main issue is to determine where we can say that a service provider had 'effective awareness'. This provision states that it occurs when a competent body has declared the unlawfulness of the content, ordered its take-down and the service provider knew about such legal decision. The requirement of the 'effective awareness or knowledge' was also established in the Directive[1940], but it permits Member States to decide the possibility of introducing specific requirements, such as duties of care. There is a duty of collaboration of the service providers when a competent body decides to take down or stop the provision of a service[1941]. In that case, the service providers may be obliged to take down the intermediary service used to provide the service. However, even if Member States can establish a duty of collaboration or communication for service providers, it is not mandatory to monitor the data that is hosted in their services, nor actively search for circumstances that may indicate illicit activities[1942], as it is stated in the Directive.[1943] Hence, we can say that the internet intermediaries will be subject to the general rules of Spanish liability, and, additionally, to these specific rules that are established in the LSSI, which are a transposition of the Directive on electronic commerce. Nonetheless, these provisions establish a framework for a liability exclusion, more than an actual liability regime.[1944] If it is proved that the actions of the service providers do not fall under the scope of the liability exclusion, we will then have to establish which are the applicable liability rules. In this case we would be subject to non-contractual liability, which takes us to the Spanish Civil Code, more specifically to Article 1902 CC – civil liability of third parties – as well as to the Law for the protection of consumers and users (TR-LGDCU).[1945]

1937 Article 15. of the Information Society Services and Electronic Commerce Act.
1938 Article 16. of the Information Society Services and Electronic Commerce Act.
1939 Article 17. of the Information Society Services and Electronic Commerce Act.
1940 Directive on electronic commerce (46).
1941 Article 11. of the Information Society Services and Electronic Commerce Act.
1942 Directive on electronic commerce, Article 15.
1943 Javier Maestre Rodríguez, 'The liability of information society service providers and the new concept of public'(2017) 49 Revista Derecho y Sociedad.
1944 Miguel Peguera Poch, The exclusion of liability of internet intermediaries (COMARES, 2007) 292.
1945 Roberto Yanguas Gómez, *Internet connexion contracts, "hosting" and searches* (1st. Edn, Aranzadi, 2012) 426.

In terms of the criminal liability, by virtue of Article 30 of the Spanish Criminal Code, the liability of information society service providers is always subsidiary to that of the author of the illegal content, whose dissemination constitutes a criminal breach. Nevertheless, this precept expressly refers to mechanical means of dissemination. Due to this wording part of the legal doctrine deems that this Article is not of application to information society services providers and thus their responsibility will depend on their categorisation of this provider into either author or participant. As a consequence, the liability of the cited provider requires a personal development or cooperation of the unlawful content, excluding those providers that merely facilitate the service as they do not have an effective awareness of the facts. If on the contrary the internet intermediary had an effective awareness or knowledge of such content, he will be liable for the crime committed by the author.[1946] With regard to restrictions to the freedom to provide services, such as blocking or taking down content, the Directive states that it is not mandatory for intermediaries to control the information that is hosted in their services[1947]. However, intermediaries will be liable when they have effective awareness of illegal content hosted in their servers and they did not take-down the content or block it. Additionally, the Directive leaves at the discretion of Member States the establishment of obligations for intermediaries to inform public authorities of illegal activities or information hosted at their servers.[1948] In the Spain legislation there is a provision in Article 8 of the LSSI that allows competent administrations to implement measures to take down or stop the provision of content that violates certain principles. Some of those would be the safeguard of public order; protection of public health, consumers and users; dignity, non-discrimination principle; infant protection and intellectual property safety.[1949]

[1946] Susana Navas Navarro y Sandra Camacho Clavijo, Digital Market- Legal principles and rules (Tirant lo Blanch, 2016) 135.
[1947] Directive on electronic commerce, Article 15.
[1948] ibid.
[1949] LSSI, Article 8.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1 Actors at a national level

Apart from EU rules and norms, there are various national actors that will drive the change at a national level both in terms of the law-making process and the application or interpretation of the provisions adopted in the three matters that are covered in this question. Their role will be analysed in the sections below. In accordance with the influence that their legal reports, bills and decisions have in law-making, the actors are the following:

— Administrative organs:

- Spanish Data Protection Agency (AEPD)
- Regional control authorities in the field of Data Protection: located in Catalonia, Basque Country and Andalusia.

— Central government

— Judiciary

7.2 Right to be Forgotten

When it comes to the number of requests to remove content, even since the decision of CJEU in 2014, Spain has a record of a total of 78.893 requests, placing Spain 5th in the ranking of European Countries that have received a bigger number of claims. Requests filed by natural persons' account for 88,6% of all requests, thus making an issue of public importance. Yet the Spanish legislator is not taking proactive steps to shed light to this right, leaving it to the Spanish Data Protection Agency and the jurisprudence of the courts of law, (national courts but fundamentally the CJEU) to delimit this right. Therefore, the future developments in this regard are likely to come from the judicial review of the Luxembourg Court and the task of interpretation and execution of the Spanish Data Protection Regulation entrusted to the Spanish Data Protection Agency (hereinafter AEPD).

In this regard, the AEPD has elaborated a number of guides and legal reports to guide the data subjects and controllers of the correct implementation of Data Protection Rules. An important guide has been elaborated on Artificial Intelligence, which tackled the right to erasure of data that resulted from an AI

process. In this regard the AEPD has set the basis for its application, stating that if the model contains incorrect personal data that can lead to a identification of the data subject, it is necessary to take down this false content, as it is erroneous. However, the guide expressly foresees the possibility of data pertaining to the model which does not have an effect over the individual, for instance for having no link of the erroneous information with the data subject. In such an event, the right to be forgotten shall be applicable. As a result, the AEPD opens the way for controllers of treatments of data through AI techniques to make use of an strategy to abstraction and concealment so as to guarantee the data minimisation principle.[1950] Furthermore, a further conflict has arisen recently over the emerging technologies. This problem revolves around the immutable character of Blockchain technology. There is a great debate over such nature in the Spanish Academia, but the Spanish legislation seems to not be suited for this rapid change. Blockchain has a huge potential to transform business models, and in particular the financial sector and contractual relations, through the so-called smart contracts. As a consequence, the investment carried out by Spanish firms in these technologies, including certain law firms, has exponentially grown, yet the compatibility of the Data Protection legislation in force with these features of the Blockchain technology is at doubt.

A possible solution to this conflict is the limitation of the scope of this right in the distributed ledger systems, in such a way that it would suffice with the non-accessibility of the data that is to be forgotten and it would not be necessary to suppress the data. This is a solution that the Spanish legislator has on its hands. On the other hand, another solution would be the development of an editable Blockchain, where the characteristic of the immutability is no longer present. This development would entail the possibility of changing blocks without altering the whole chain, which is not currently possible.[1951] Nevertheless, this solution lies in the endeavours of the actors in this industry to modify the functioning of the distributed ledger so as to adequately address the fundamental right of the Right to be Forgotten.

Another issue that will certainly influence the development of the Right to be Forgotten is the state of Freedom of Expression in the case law and legislation. There has been a heated debate in our country over the degree of tolerance that should be granted to expressions that express nostalgia or praise towards the

[1950] Spanish Data Protection Agency, Adaptation of treatments of Data that introduce AI to GDPR , February 2020. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf Accessed 22 February 2020

[1951] Ministry of Industry,Commerce and Tourism & RED.es, Digital Society and Law (Official Bulletin of the State, 2018)

Francoist regime (1936-1975). The current government has expressed its intention to categorise as a crime the incitements of the Franco regime. Such an issue at stake, requires a necessary balance between Freedom of Expression and the protection of the victims of such regime, mainly dissents and oppressed activities during the Franco era until 1975. This issue has reached the AEPD. On 2019 an enquiry was addressed to the legal department of this agency, over the suitability of the data protection legislation with the work named 'Francoist Criminal Law and Homosexuality: from sin and outrage to the state of danger' that the Ministry of Justice intended to publish. This work includes names, surnames and other personal details of judges, forensic doctors and other civil servants that were present in judicial proceedings where the accused were persecuted due to their sexual orientation, in the application of the criminal legislation in force at the moment. The enquiry deals with the appropriateness to publish the personal data of such data subjects acting under the capacity of public authorities, without the need of obtaining the consent of such subject or that of their heirs in the event that those data subjects no longer lived. The Agency deemed that the publication of the personal data of such subjects is not contrary to the data protection law, as it concerns a historic investigation and the data corresponds to subjects exercising public duties and functions. As a result, the right to be forgotten was not acknowledged.[1952] The report by the AEPD referred to the ruling of the Constitutional Court no. 28/1982 where the Court declared that judicial proceedings that were adjudicated during the Spanish Civil War (1936-1939) present an 'unquestionable public relevance' as they reflect historical facts and tragedies that shaped the realities of such an era. Scientific freedom enjoys an increased protection in those cases in relation to Freedom of Expression and Information. While Freedom of Expression and Information refers to actual facts carried out by people at the present, scientific freedom refers to past facts, characterised by individuals whose personalities have faded in history.[1953]

There is a public debate over Freedom of Expression of symbols and other expressions that can be identified with the Francoist era. On the other hand, there is a sector in the political spectrum that advocate for the categorisation as crime of such expressions while another sector sustain that the criminal intervention is not an effective response to dissuade and prevent the spread of authoritarian expression that identify with fascist regimes. This debate will have an impact over the application of the Right to be Forgotten, while contributing to an increased liability of internet intermediaries, and an eventual obligation to

[1952] Spanish Data Protection Agency, Report no. 2019-0044 emitted on 18th of March 2019.
[1953] Judgement of the Constitutional Court 28/1982, de 26 de mayo [RTC 1982, 28] , F. 2.

prevent such incitements. The issue at stake will undoubtedly influence internet governance in our national legal order, but whether this heated debate constitutes a strategy of the government so as to create a smoke screen, or on the contrary contributes to a development in other aspects of Freedom of Expression on the internet remains to be seen.

7.3 Liability of internet intermediaries

At this point it is important to take a look at the recent developments made internationally. The recent sentences regarding this subject by the European Court of Human Rights *Defi As vs. Estonia* and *Magyar Tartalomszolgáltatók Egyesülete y Index.hu Zrt vs. Hungary* do give us an insight into what the future of internet intermediaries' liability could look like. Both sentences treat the subject in a different way, depending on the affected person. The key difference between those two cases is that, on one hand, the aggravated subject in *Delfi As vs. Estonia* is a physical person, which suffers because of the hate comments made on one of the most influential news websites of Estonia. The Court appreciates the responsibility of the website's owner, even though the comments were posted by other people on the website.

On the other hand, in *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt vs. Hungary* the aggravated subject is a juridical person instead of a physical one. A Hungarian enterprise sees its name damaged because of the comments and news published on the applicants' website. These websites both clarify that they aren't responsible for the posted comments nor do they reflect their opinion, although the Hungarian Courts did make them responsible. What's more, both have a notice-and-takedown system in place, regulating to some extent the posted comments. The European Court of Human Rights decided that this was enough in this case, given that the comments (as opposed to the *Delfi As vs. Estonia* case) weren't constituent of hate speech. Therefore, the Government could not hold the applicants accountable for the comments, in favour of liberty of speech.

After analysing these two sentences, we can envisage the enlargements of the liability of internet intermediaries in our national legal order, due to the big influence that the case law of the ECtHR has in our law-making process. This criterion that has been established by the ECtHR is only an example of a doctrinal line in various jurisdiction that propels the imposition to intermediaries of obligations to the active supervision so as to prevent illegal content from being published, thereby creating a progressive separation from the pre-existent criteria not to impose obligations of supervisions to online content providers under the Information Society Services Act. Nevertheless, there is a high dissent of this doctrinal line in our case law. Thus, we can find other rulings that

acknowledge and strengthen the pre-existent responsibility regime. This conflict arises from the difficulty that has emerged with fitting the big digital platforms into internet service providers or intermediaries. The transformation of the digital economy into an economy of platforms has led to a high doubtfulness of the legal regime that is applied to these platforms, either that of Internet Service Providers or that of intermediaries.[1954]

Our current paradigm, set out in Articles 12 to 15 of the Electronic Commerce Directive, consists on the prohibition to impose intermediaries' general obligation to supervise or carry out the search of facts or conditions that might reveal unlawful activities on the one hand, and a subjective liability system on the other hand, whereby the factor that triggers the liability of the intermediary is the effective knowledge. Only the existence of this effective knowledge creates the obligation on the intermediary to take down or block unlawful internet content.

Evidence of this increased responsibility of intermediaries can be seen in the wording of the political programme of the party that is currently the government, which states 'the exponential growth of big technological companies, with a big amount of market power and social influence, make it necessary for an adjustment of our institutional architecture so as to guarantee a minimum level playing field where there is fair competition and the public interests are safeguarded. As a result, it is necessary to update the policies of supervision of the digital market, competition policies, the taxation system and data protection'. This statement reflects the will of the government to put constraints on the intermediaries in order to minimise a position of dominance that many of them possess in the market. Example of this is the newly adopted so-called 'google fee'. Either through fiscal measures or through data protection, the public authorities will exercise a more intense supervision and policing role vis-à-vis internet intermediaries.

An example of this increased liability can be found in the newly adopted Directive 2019/790 and its controversial Article 17 which has alarmed social networks users and, above all, online content creators. This Article establishes that the Internet intermediaries will no longer be able to benefit from the operational liability exemption regime, so they will be obliged to acquire a license to respect IPR or, alternatively, to make their best efforts to guarantee this

[1954] Ministry of Industry,Commerce and Tourism & RED.es, Digital Society and Law (Official Bulletin of the State, 2018) Chapter elaborated by Teresa Rodríguez de las Heras Ballell, The trust in in the digital society: the function of intermediaries and reputational systems.

provision. This is quite similar to the accountability principle regarding the EU Data Protection.[1955]

But the presence of algorithms which detect and remove IP infringements or illegal content on the Internet is the order of the day for a couple of years. The implementation of them in social networks has had pernicious effects. Many of these content creators, most of them singers, have abandoned the famous social network YouTube for others less restrictive, in order to avoid the removal of all their content for infringing IPR. One of the first famous cases in Spain was Alissa, she did covers of the Spanish singer Pablo Alborán using the original musical base of the artist. Therefore, YouTube required her in September 2017 to delete all of her videos[1956]. Nevertheless, the effectiveness of these algorithms is very controversial. Some examples have taken place in Spain, as the photo of a typical 'cocido' (stew) posted on Instagram which have been removed for containing violent material[1957].

There are all signs of change, that seem to indicate a new paradigm of an increased responsibility of intermediaries in the prevention of unlawful acts and the protection of different rights. The most expected scenario is thus one were the internet intermediary and the person which comments or takes action as such are held responsible in a solidary manner.

7.4 Current context

What is the positioning of the current government in these issues? In order to know the stance of this fundamental actor, it is important to turn to the electoral programme with which the government was elected through parliament and the government programme. The Socialist party, the party that is currently at the government, included in its electoral programme a section that tackles with the challenges digitalisation, outlining the policies it advocates for. In light of this document the current government is putting a special focus on the worker's rights and the rights of the child in cyberspace. As a result, they have expressed their intention to impulse a right to digital disconnection for civil servants as well as the elaboration of a bill that guarantees the rights of the child on the internet,

1955 El Condifencial, the present and the future of responsibility in the internet https://blogs.elconfidencial.com/espana/blog-fide/2019-07-04/presente-futuro-responsabilidad-internet_2100434/ Accessed 18 February 2020.

1956 Los 40, " the woman that did versions of Pablo Alboran had the obligation to erase such content" https://los40.com/los40/2017/09/01/tecnologia/1504260082_730300.html Accessed 18 February2020.

1957 La Vanguardia, Instagram considers as graphic violence the pictures of a graphic stew and blocks them https://www.lavanguardia.com/vida/20191022/471143662208/richard-barreira-instagram-elimina-fotos-cocido-gallego.html Accessed 20 February 2020.

with the purpose of safeguarding their security. The content of these new rights is to be essential for the takedown and blocking of internet content.

In the coalition government programme, it is expressly set out as one of the objectives of the current government the adoption of a Digital Rights Act which is to develop the pre-existent rights present in the Organic Law of Data Protection and Guarantee of Digital Rights. This law set out a mandate for the Central Government in conjunction with the sub state governments on Article 97 consistent on the adoption of an Action Plan. This action plan is mainly aimed at overcoming digital gaps and guaranteeing internet access to vulnerable groups or groups under social exclusion. This objective is to be achieved, among other measures, through what has been called *'social check of internet access'*. Another of the fundamental targets that this Action Plan has is the fostering of educational measures for the promotion of training in digital competencies and skills from a young age and to overall society, building up capacities for an autonomous and responsible usage of these technologies.

Essentially, the Action Plan will have the function of implementing Title X of the Organic Law of Data Protection and Guarantee of Digital Rights, relative to digital rights, in the public administration and translating such rights into concrete policies. This Title was introduced in the Bill introduced by the Socialist Government, which was not present in the bill of the prior Christian Democrat government. The introduction of this section had as an objective the adaptation of fundamental rights to the new internet era and to the digital challenges and risks that harmed the fundamental rights in the Spanish Constitution. As a reform of the Constitution is not wished by the Government, both the current executive and the prior one, the introduction of a section in an Organic Law, the modality of legislation that enjoys the highest position after the constitution, was considered more suitable. The mandate to adopt this Action Plan had a time limit of a year, a limit that has been breached due to the period of time with an acting government.

The urgency for the adoption of this action makes it certain that a future development will take place in the area of digital rights. This development is likely to entail a bigger scope in the liability of intermediaries coupled with a more intense public intervention and supervision in notice and takedown procedures of online harmful content. The Spanish Government has defended at a supranational level, that the self-regulation of social networks has proved insufficient to tackle disinformation and has advocated for the elaboration of new European rules on the matter. Juan Aristegui, the Spanish permanent ambassador to the EU, has stated that the self-regulation of digital platforms

does not grant the necessary safeguards for the defence of the rights of the users.[1958]

Due to the cross-border nature of this issue Spain is acting at a supranational level in order to reach a solution on the problem of disinformation and cyber threats. The future developments that will take place as a supranational level are vital, as a big part of the developments in the field of the notice and takedown procedure will emanate from an EU level, obliging the Spanish legislator to transpose the content of directives. For instance, the ePrivacy Directive is to be adopted in the next few months, which will condition the direction of the Spanish Legislation on the matter. Nevertheless, the aforementioned factors will be essential for the transposition of the directive into the Spanish legal system.

Spain stands up for a bigger assumption of responsibility by these digital platforms, due to the role these platforms can play in disinformation. Nevertheless, this increased liability is not to be coupled with bigger self-regulation capacities but rather through a more intense supervision by the public authorities. In light of the trends that have been explained above the Public Administration is likely to play a more active role in establishing obligations to intermediaries and in safeguarding the rights of the users. The current government is defending these policies both at the national institutional level and at a supranational level.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

With the emergence of social groups and political parties with intolerant and discriminatory discourses that put into question the democratic values, the risk of hate speech has been made more apparent. Nevertheless, the need to face these discourses has shown a restrictive tendency of Freedom of Expression. The so-called crimes of opinion have emerged in our national legislation, with the basis that there are certain expressions or discourses that due to their content should not be tolerated in the public sphere. As Rosenfend explains, new approaches have arisen that put a focus on the way Freedom of Expression can affect the autonomy and dignity of the members that form part of vulnerable

[1958] Europapress, Spain considers self-regulation of social netowrks insufficient to tackle disinformation https://www.europapress.es/sociedad/noticia-espana-ve-insuficiente-autorregulacion-redes-sociales-atajar-desinformacion-20190523142920.html Accessed 18 February 2020.

groups or minorities, who can be exposed to dominant discourses that exclude them. Nevertheless, as other authors have pointed out, it is important to keep in mind in this balancing act with hate speech that Freedom of Expression consists of the freedom of breaking with the established patterns of thinking through expressions and speech. It is thus the most fundamental freedom citizens have in a democratic society, which leaves room for the political dissent, for the transgression. It therefore has a clear dimension of right of defence. In order to express neutral ideas or ideas that are in accordance with the common values of a society, Freedom of Expression is not needed, but this right is rather needed to challenge these values. Freedom of Expression and Information is above all a Right of Defence. The balance between the two above mentioned versions, might be altered as a result of the widening of the scope of hate speech as a limitation to this freedom. The well-meaning and necessary protection of social groups through the punishment of certain discourses can turn to imply an institutionalisation of Freedom of Expression, hampering its nature of Right of Defence.[1959] The Spanish constitutional order in terms of Freedom of Expression has been defined as an open and personalist system. As a result, in order to justify a limitation of the Right to Freedom of Expression it must be justified the effective injury or risk of a legal good. The Court has enshrined the harm principle. This principle makes it necessary to distinguish those expressions whose restriction will be legitimate due to an effective damage to legal goods, from other expressions that, even if they shock, disturb or offend, do not acquire the sufficient gravity to be restricted.

The open and personalist constitutional order in force, is very far from what the Constitutional Court has named as the 'model of militant democracy'. Nevertheless, in the case law of this Court elements of functionalisation of this right can also be found in cases concerning digital technologies, whereby the Court deprives protection to expressions contrary to the values of society, which had the consideration of hate speech. Following the Supreme Court case law, new technologies intensify exponentially the damage of affirmations or messages which, at another time, could have limited their harmful effects to a small and selected group in perpetuity[1960]. This position can be considered to be disproportionate because, even if the messages on the Internet can potentially reach many people, only a specific analysis of each case allows us to conclude if

[1959] German M teruel Lozano, When words generate hatred: limits to freedom of expression in the Spanish Constitutional Order (University of Murcia, 2018).

[1960] Judgement of Supreme Court No. 4/2017 of the 18th of January, 2017.

it reached a remarkable diffusion.[1961] As a result, it denotes a fearful approach to the digital era.

The criminal courts have ordered the removal of content on the Internet because the manifestations reproduced was a criminal offense of glorifying terrorism. Some tweets were considered as an incitement to violence, as they praise terrorist groups, and they were also published for an extended period of time[1962]. Moreover, songs published on social media have been taken down for similar reasons[1963], in particular for being an incitement to terrorism, as they mentioned and glorified terrorist groups in its lyrics. In other situation[1964], tweets and songs were removed as being a glorification and justification of terrorist crimes committed in Spain, being an act of humiliation of terrorism victims and their families. They are removed because they go beyond the expression of solidarity with the prisoners or political support, the violent means used, and the repetition of the comments are not protected by the Freedom of Expression. Likewise, there were expressions which exceeded the political criticism, attacking on the reputation and honourability of the King of Spain and charging with inexistent crimes. Also, they contained insults or serious threats for the Spanish Army and National Security Forces.

8.1. Protection of Hate Speech under Criminal Law

Hate Speech has been defined as: 'all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin'.*[1965]*In order to categorise a message as 'hate speech' it has to fulfil some requisites. One of these is the public nature of such messages. In some Articles it is clearly stated, while in others it can be deduced from the legal text.

The first requisite is the publicity of the hate speech. The Spanish Criminal Code regulates in Articles 510 and 578 the publicity requisite. In these Articles, the legislator refers to hate messages towards minority groups and messages exalting terrorist activities, which are also considered hate speeches. The main idea is

---

1961 TERUEL LOZANO, G.M, "Intolerant expressions, hate crimes and freedom of expression: a difficult balance", Legal Journal of the Universidad Autónoma de Madrid, No. 36, 2017-II, page 194.

1962 Judgement of the High National Court (Criminal Chamber, Section 1) No. 4/2018 of July 10th, 2018.

1963 Judgement of the High National Court (Criminal Chamber, Section 1) No. 6/2018 of the 18th of September, 2018.

1964 Judgement of the High National Court (Criminal Chamber, Section 1) No. 3/2018 the 2nd of March, 2018.

1965 Council of Europe, 'Recommendation No. R (97) 20 of the 30th of October 1997 of the Committee of Ministers to member states on "hate speech".

what is understood as a 'publicly expression'. The Council of Europe defines it in its Convention on the Prevention of Terrorism as the 'the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.' Therefore, a message will be a public expression whenever it is made available to the public. In certain Articles, the word 'publicly' is not used. Nonetheless, it can be deduced from its context that the actions mentioned in such Articles - 510.1.b) and 510.2.a) - require the message to be publicly spread. The second requisite, is negatively defined, that is to say, it is not necessary that the issuer is the author of the message. As a consequence, being a third party that spreads a hate message is a crime, just as it is being the author of such a message. An example would be the person that writes a tweet (author) and another user that retweets it, and, thus, disseminates it. In these cases, we are assuming that the communication is public, regardless of the number of people who could have read, listened or watch the information, because the message aimed at a great number of potential recipients. As a consequence, a private message, i.e. a person sending a message individually to another person, containing hate expression is not considered a crime because of the lack of publicity.

Due to the proliferation of social networks, questions regarding this publicity requisite have arisen. On the internet, it is possible to write a private message to more than just one person, because of the nature of social networks. However, what has to be considered is not the number of people who receive the message, unless the potential recipient is extremely high, because the difference between a public and a private message is qualitative. In order to be a private communication, the sender has to know the identities of all the recipients who are going to receive the message.[1966] In light of the increased risks, hate speech is aggravated when it is diffused on the Internet, according to Article 510 (3) of Spanish Penal Code, because they are accessible to many people. Likewise, social media increases the commission of these illegal acts, as the communication is with immediate effect and it is possible to comment anonymously. Many users have found a way to make their political demands or even to express their feelings about current situations. To this extent, the Spanish Supreme Court has stated, as it was mentioned above, that the New Technologies intensifies the harm of this kind of messages, given the fact that there are more recipients, they

[1966] Jaime Goyena Huerta, Some criminal matters on hate speech. (Aranzadi Journal on Law and Criminal Procedure no. 49/2018). .

can become permanent and its author lacks control of its diffusion.[1967] The Supreme Court is therefore adopting a fearful approach to digital reality in its reasoning. In this digital context, there are four requisites so that a message is considered non-publicly expressed: i) the recipient group cannot be conformed by a large number of individuals; ii) the access to the group is restricted; iii) the sender knows the identity of all recipients; iv) the sender is not aiming to spread the message beyond that group. Therefore, what is most decisive to qualify a message as private is the trust between the individuals participating in the conversation.[1968]

Thus, a tweet could be considered in this framework of Article 510.3, even if it is posted in a restricted-access group; whereas a WhatsApp message sent in a private group would not fall into this scope, because it would be a closed group and the sender knows all the recipients.

Not all the messages of hate must be considered as hate speech and this has been really controversial in Spain in the last years[1969]That is why Spanish case law is very little related to this crime. On many occasions, these messages do not usually reach the seriousness required by Spanish Courts. For example, the animation about twenty ways for a woman to die uploaded on a Political Party website is not hate speech, because they used 'die' and not 'kill.'[1970] Recently, tweets published by a Constitutional Law Professor, where there were threats to public servants, prosecutors and judges for having extorted Catalonia and an incitement to violence to reach independence, were not considered as hate speech as they were not sufficiently explicit to be a real danger.[1971]

Nevertheless, the classical means of communications do not have the same broadness as the ones that exist nowadays, because with the Internet a message can become viral in just a few hours, and such facts must be taken into consideration. That is why our Penal Code establishes a criterion of 'uncontrolled spread', which is included in Article 510.3. There are two requisites to consider a message of such nature: being spread through the Internet and that the message is available to a large number of people.

1967 Judgment of the Constitutional Court 4/2017, de 18 de enero, FJ. 2.

1968 Jaime Goyena Huerta, Some criminal matters on hate speech. (Aranzadi Journal on Law and Criminal Procedure no. 49/2018).

1969 TAMARIT SUMALLA, J.M., "Hate speech crimes in social networks" Internat, Law and Politics Journal N.º 27 (Septiembre, 2018), pp. 22-23.

1970 Judgement of the Provincial Court of the Balear Islands (Section 1ª)Ruling no. 312/2013 of the 10th of December.

1971 Judgement of the Provincial Court of Barcelone (Section 8ª) Ruling no. 607/2018 of the 7th of December.

Hate speech crimes because of racism or xenophobia are the most common. The video uploaded on Facebook entitled 'Kill all the Jewish' is one of the examples;[1972] In this one two women stabbed a knife in a doll with a photo of three Jews minors who were kidnapped and killed. Another case is the commentaries uploaded on Facebook groups containing discriminatory and humiliating expressions about Moroccans; specifically, the offender wanted them dead from drowning or burning just for being in this country.[1973] Case law of this crime can be also found in messages containing gender hatred. One example is a Twitter user with 2.000 followers who published some aggressive tweets on gender lines stating that more women should be killed by men.

As a consequence, protected subjects by hate of speech crimes are vulnerable minorities, such as immigrants, homosexuals or marginalised groups, as well as jews, as it is established in the previously mentioned Recommendation[1974] of the Council of Europe. That is why the criminal regulation of hate speech in force criminalises those expressions or discourses related to gender, ideological, racial and xenophobic hatred. The legal doctrine has stated that this Article lacks determination and, consequently, it generates an undoubted deterrent effect on the legitimate exercise of Freedom of Expression.[1975] One example is the extensive consideration of this crime by the Constitutional Court in this Judgement No. 177/2015, when it was considered as hate speech the burning of a portrait of the Kings of Spain in an anti-monarchist manifestation.[1976] This judgement was lately annulled because the ECHR understood that this manifestation could not have been considered as hate speech, because there is not an incitement to hatred and violence.[1977] The glorification of terrorism and the humiliation to terrorism victims cannot be recognised as hate speech because it is related to Freedom of Expression and that is why it is regulated in other part of Criminal Code (Articles 576 and 578).[1978] However, the Spanish legislator uses an open formula, whereby all hate speeches have the same passive subject: a group or a person who belongs to that group. The main objective is to offer a broader protection, because the legislator lists the actions that may become a hate crime, while at the same time the protected subject is broader than the one established in the Recommendation.

1972 Judgment of the Provincial Court of Navarre (Section 2ª) Ruling no. 55/2017 of 21st of March.
1973 Judgment of the Provincial Court of Barcelone (Section 10ª) Rulin no. 299/2019 of 21st of May.
1974 Council of Europe, 'Recommendation No. R (97) 20 of 30 October 1997 of the Committee of Ministers to member states on hate speech.
1975 Teruel Lozano, G.M, "Intolerant expressions, hate crimes and freedom of expression: a difficult balance", Legal Journal of the Universidad Autónoma de Madrid, No. 36, 2017-II, page 187.
1976 Judgment of the Constitutional Court No. 177/2015, of July 22nd, 2015.
1977 *Case of Stern Taulats And Roura Capellera v. Spain*, Judgment of ECHR (3d Section) of 13 March 2018.
1978 Judgment of the Constitutional Court 112/2016.

8.2 Parameters for the balancing between freedom of expression and hate speech

Despite this protection, Freedom of Expression has to be protected within the established framework, but not every message that exceeds the limits has to be identified as a crime[1979], because our legal system has other mechanisms to deal with possible hate messages, i.e. administrative sanctions. It is necessary to identify the type of speech, because there are different criteria for the different kinds of speech. For example, it is not the same opinion Article in a newspaper than an artistic creation such as a novel, a poem, a film or a song.

A field that is especially controversial is humour, which sometimes is sarcastic or dark. Humour itself usually is based on race, nationality, religion or sex. However, the limit has to be considered depending on the context: who tells a joke, when, where and how. Therefore, the same joke can be a crime under certain circumstances, but not in a different context.

One of most essential parameters that are used is that the expression constitutes a contribution to the formation of public opinion. In the absence of this requirement it is deemed that that the expression is incompatible with the system of values of democracy. This parameter was introduced in the ruling of the Constitutional Court, where the court held that a comic was in direct contradiction with the principles of a democratic system, essentially those related to the protection of the child.[1980]

Initially the Constitutional Court identified hate speech with those expressions or manifestations of racist, xenophobic or discriminatory character that directly incite the violence against certain races or minorities. Nevertheless, lately the Court has extended this definition to come to include as hate speech the mere intolerant discourse. In the ruling of the Constitutional Court 177/2015[1981], the category of hate speech was extended beyond the forms that are merely projected over the ethnic, religious, cultural or sexual conditions of persons, including more alternatives into the concept of hate speech, namely that of the 'fobic discourse' which consists on the promotion of exclusion or rejection from politic life and the physical elimination of those who do not share the ideals of the intolerants.[1982]

[1979] Judgement of Supreme Court No. 4/2017 of the 18th of Fed, 2017.
[1980] Judgment of the Constitutional Court 176/1995, of the 11th of December.
[1981] Judgment of the Constitutional Court 177/2015, of 22 of July.
[1982] German M teruel Lozano, When words generate hatred: limits to freedom of expression in the Spanish Constitutional Order (University of Murcia, 2018).

The broadening of the scope of hate speech can be observed in a case that reached the ECtHR. The Constitutional Court condemned the applicant for injury to the Head of State for the burning of portraits of the King of Spain. The ECtHR ruled that such facts cannot be considered as a form of hate speech or incitement to violence. This ruling has fuelled the debate in the doctrine. Certain judges have expressed the banalisation of hate speech, among which we can find the dissenting vote submitted by judge Juan Antonio Xiol in the sentence pronounced by the Constitutional Court in the cited case. In this dissenting vote, such a judge declared that the interpretation made by the sentence not only did it lack the factual basis but it also distorts or denatures the concept of hate speech. Alcacer Guirao has also criticised this conceptual drive, stating that the concept of hate speech is now identified with the mere manifestation of hostility.

In the conflict between hate speech and Freedom of Expression, other rights come into play mainly the Right to the Protection of Private Life, reinforced with legal goods such as human dignity and the prohibition of discrimination. These latter goods had initially a personalist conception by the Constitutional Court but have however acquired a collective character. Firstly, the Court lowered the threshold for the protection against insults, protecting not only insults that are addressed to persons that are individually considered but also insults that are addressed to persons who are not perfectly individually considered in a perfect or due manner but are carried out in a generic or imprecise manner. Secondly, the condition of passive subjects has been recognised by social groups. As a consequence, the protection of private life has obtained a collective dimension.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

The fundamental rights specifically stated in Article 20.4 CE are considered as external limits to the Freedom of Information. Thus, in the Ruling of the Constitutional Court 23/2010, of the 27th of April, FJ 3, the cited Court had reiterated that 'section 4 of Article 20 CE stipulates that the freedoms recognised in the rule have their limit in the right to honour, to privacy to freedom from injury to reputation, honour or feeling and to protection of youth and childhood, which play what we have called a 'limiter function' with regard to said freedoms'. Additionally, the Spanish Constitutional Court has noted that, 'the right to communicate and broadcast reliable information does not grant holders an unlimited power over any scope of reality. It can only, since it is acknowledged

as a means of shaping public opinion, legitimise the intrusions in other fundamental rights which are consistent with the stated purpose, lacking legitimising effect when it is exercised in a disproportionate and excessive way with regard to the purpose in reference to which the Constitution gives it special protection'[1983], or that, 'in those cases in which, even though an intrusion in privacy occurs, such intrusion shows itself to be necessary to achieve a constitutionally legitimate purpose, provided to achieve it and it is carried out using the necessary means to assure the least affectation of the field guaranteed by this right, it could not be considered illegitimate'[1984]In light of the above, the intrusion in the fundamental rights of third parties resulting from the exercise of the Freedom of Information will only be legitimate to the extent that the affectation of such rights is appropriate, necessary and proportionate for the constitutional realisation of the Freedom of Information. Therefore, Freedom of Expression or Information will prevail where it is possible to access the information sought without the need to conflict with said rights, the information activity which unnecessarily invades the privacy or the reputation, honour or feeling of others for being excessive or disproportionate is made illegitimate. We will now assess the different rights that constitute a limitation to Freedom of Expression and the proper balancing act between those rights and Freedom of Expression.

9.1 Right to respect for private life

The development of electronic communications technologies and the internet has provoked a drastic change in the understanding of communication. This change pushed the reformulation of the traditional conception of the Right to Privacy and new mechanisms of protection. It has been in the context of the internet where the intrusions in the private sphere of the individual have exponentially increased, leading to a clash of Freedom of Expression and the legitimate interests of the users for the access to the data with the right for the protection of private life. In order to respond to this clash with the usage of ICT technologies, the Right to Digital Privacy or the Right to Computer Freedom (*liberté informatique or libertad de información*) has been created, whose main expression is the right to remain anonymous in the internet communications. This right consists on the power to control the personal identity on the web through active consent. Consequently, with technological development and the emergence of ICT technologies the concept of private life has evolved over time. Previously, it was defined as the right of not being the object of an illegitimate

[1983] Judgment of the Constitutional Court 185/2002, of the 14th of October, FJ 3.
[1984] Judgment of the Constitutional Court 156/2001, of 2 July, FJ 4.

interference in the private and familiar sphere of the individual without its authorisation. But currently the concept does not only include the right not to be subject to intrusion, but it also encompasses the right to control the usage that others do of information that reveals fundamental aspects of our private life. As the Constitutional Court has held in the ruling 176/2013, Article 18(1), relative to the Right to Privacy, guarantees the decision of maintaining secret aspects of our lives that we deem its secrecy as most suitable. It is completely forbidden for third parties to define the edges or limits of our private life. Moreover, in terms of the relationship of this right with Freedom of Expression, in the internet age it is considered that respect for private life is a necessary prerequisite for the enjoyment of other rights such as freedom of thought, political ideas, etc. This essential nature along with its consideration as right to control of information, entails that as a general rule in the event of an intrusion into the private sphere, the Right to the Protection of Privacy prevails over Freedom of Expression. It is closely linked to the free development of personality, and therefore it is not possible to maintain a minimum standard of living with the deprivation of this right.

For the delimitation of the reserved ambit or sphere of privacy, the actions of the individuals are determinant by virtue of Article 2.1 of the Civil Protection of the Right to Privacy Act. If a person relinquishes through its acts certain aspects of his private life, this publicity or transfer will be determinant for the delimitation of the sphere of privacy, so much so that the information that make reference to the aspects of the life that have been relinquished will not be considered as an intrusion into the private sphere of the individual.

In the field of Criminal Law, the protection of the private sphere has as its representation the crime of defamation. This crime has as its legal goods human dignity and public reputation. Its definition is set out in Article 208 of the Criminal Code by virtue of which 'defamation is the action or expression that harms the dignity of another person, detracting from his reputation or attacking his self-esteem,' and that according to Article 209, 'severe defamation perpetrated with publicity shall be punished with the penalty of a fine from six to fourteen months and, otherwise, with that of three to seven months,' posing an impassable limit on Freedom of Expression.

9.2 Data Protection Rights

Paragraph 4 of Article 18 of the Spanish Constitution establishes a generic mandate for the Spanish legislator to limit the usage of information technologies to safeguard the personality rights inherent to the private sphere of the user. This mandate can be sustained over the risk of an intrusion into the private life due

to the accumulation big influx of `personal data. Through this mandate the legislator has passed the Data Protection Legislation. The *raison d'être* of Right to the Protection of Personal Data consists of safeguarding the capacity of the individual to control their personal data. Essentially it lies on the data holder the decision to provide its personal data to the controller on the basis of the purpose for which the data is processed, as well as the verification that such data is certain and adequate for the intended purpose. In an indirect fashion, internet censorship could take place for data protection purposes, privacy and security, as in the case of Right to be Forgotten. The censorships in this case would derive from the obligation of the data controller to erase personal data in the legitimate request of the data subject. In this regard if the digital contents fulfil two elements: veracity and relevance for the public opinion, Freedom of Information prevails over the right to data protection of the data subject. While on the contrary if sufficient time has passed for it to be considered irrelevant for the formation of public opinion, the data subject will be able to exercise the right to be forgotten, which will prevail over the interest of the general public to access such information.

9.3 Protection of the child

The rights of the child constitute a limitation of Freedom of Expression by virtue of Article 20.4 of the Spanish Constitution. This limitation is aimed at granting a specific protection to these infant phases of life that need the absence of external interferences that can put a burden on the free development of the personality. The current legislation which regulates the protection of minors online is the following: in the first place, we have the previously mentioned 'Organic Law on Data Protection and Guarantee of Digital Rights' specifically section 84 of the norm. This section states that parents or tutors will ensure that minors make responsible use of digital devices and information society services to ensure the proper development of their personality and preserve their dignity. Moreover, it also states that the use or defamation of images or personal information of minors in social networks and equivalent services that may imply an illegitimate interference with their fundamental rights will provide measures regulated in the Organic Law 1/1996 of the 15 January, on the Legal Protection of Minors. Concerning the current legislation about personal data protection, section 13 of the Royal Decree 1720/2007 21 December, gives minors who are 14 years old the ability to give consent for the treatment of their data, unless the law obliges the presence of a parent or tutor. In order for this consent to be valid, section 13's third paragraph states that the information with regards to the minor's data treatment must be written in a simple way to be understood by him.

The Spanish Constitution of 1978, more specifically section 39 establishes the following: 'Children shall enjoy the protection provided for in the international agreements safeguarding their rights'. Thus, in this field we must refer to the General Data Protection Regulation where the concepts of "transparency" 'privacy by defect' 'adequate information' and 'minor protection' are the protagonists.

It is also worth mentioning the 'Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual' specifically paragraph 2 of section 7 which states the following: 'it is forbidden the emission of audiovisual content that can harm the physical, mental or moral developments of minors and in particular programs that include pornographic scenes or violence. The conditional access must enable parental control'. The cited provisions constitute safeguards for the protection of minors online. If any of these rights or provisions enter into conflict with Freedom of Information or Expression, the rights of the child prevail over Freedom of Expression online as established in the Organic Law 1/1996, de 15 de enero, on Legal Protection of the Minor.

9.4 Collective limitations

Lastly, apart from the legitimate interests of the minor, of the data subject and of the private sphere of the individual, legal goods that possess a collective nature have been introduced by the Spanish legislator. A vital example of these kinds of legal bases that constitute a limitation for Freedom of Expression, is public order. In order to preserve public order, restrictions on the Freedom of Expression have been regulated by the Criminal Code: Article 578 stipulates that 'apologism or justification by means of public expression or diffusion of the felonies [of terrorism] included in Article 571 to 577 of this Code, or of anybody who has participated in commission thereof, or in perpetrating acts that involve discredit, distain, or humiliation of the victims of terrorist offences or their relatives shall be punished with a sentence of imprisonment from one to two years.'

In order to understand this restriction, it is important to understand the factors that have led to this response of the legislator. As in the physical life, there exist complex human interaction, discourse, and behaviour to be regulated by national jurisdiction, with the digitalisation of communication and information in contemporary society, the complexity of behavioural phenomenon only multiplies, with unprecedented and unforeseen circumstances emerging rapidly and remaining unregulated by law.

The transformation of communication from real life to the virtual world challenges national legal-political regime on several grounds: as individuals are

empowered to produce and distribute information everywhere and every-time on the digital platform, the originally monopolised power of information by state and multiple media outlets become decentralised into various private actors; as digital communication and other functions take place in 'places without space,' meaning that the geographical location of a user becomes insignificant with respect to the functioned performed online (Murray 2019: 89), the concept and practice of state territoriality and national jurisdiction become negligible to a large extent; meanwhile, with the multiplication of users, producers, platform providers, and other role players on the internet, the accountability and responsibility become gradually difficult to track down. The 2016 UK Referendum and US Presidential Election demonstrated new forms of digital political activism: AstroTurfing, as defined by Mark Leiser as 'a deceptive practice often deployed by markets to create the false impression that a campaign has developed organically,' involving the employment of agents who intentionally mislead and manipulate popular sentiment into believing the advantages of a product or service by being the popular representative for the real public to follow suit. This phenomenon has transformed into forms like #fakenews. To address the pressing social needs of public regulation on the ever accelerating development of digital socio-economic interaction, Royal Decree-Law 14/2019, of the 31 October, whereby urgent measures are taken for reasons of public security in the area of digital administration, public sector contracting and telecommunications, was developed and came into effect in 2019 as a translation of normative principles of legitimate use, protection of rights and freedoms, and public order, at the digital level. However, the balance between safeguarding and surveillance could be disturbed by the statist guardianship approach to internet censorship, in stating that 'the government, on an exceptional and transitory basis, may agree on the assumption by the general state administration of direct management of or intervention in electronic communications network and services in certain exceptional cases that may affect public order, public safety or national security. This exceptional power may affect any infrastructure, associated resource or element or level of the network of service that is necessary to preserve or restore public order, public safety and national security.' (No. 14/2019). While protecting citizens from misinformation, privacy infringement, and public disorder, the original and the modification of Article 155 by the newly legislated law of 14/2019 has also been criticised as implicit state oppression on the Catalan movement of independence as a response to the overwhelming manifestation of Tsunami Democracy and other pro-independence groups, regarding its mobilisation online and discussions of a nation-state aspiration in the digital forums. In conclusion, the balance between Freedom of Expression and other rights in an internet context

has been conditioned on the political crisis that has taken place in Spain for the past three years between the Central Government and the Regional Government of Catalonia. The attempts of pro-independence groups to achieve their objectives through digital means has led the Central Governments to foresee measures that restrict the access to information in the event of situations that put at risk the territorial integrity of the State. Whether these measures are proportionate for the aims sought is constantly present in the political debate of our country. This Royal Decree has given the Central Government the right to assume direct management or to intervene in the networks and electronic communications services in exceptional cases. Nevertheless, as the specific cases that trigger this intervention have not been outlined, the definition or the delimitation of this exceptionality is left to the discretion of the said organ. This openness has been considered by wide sectors of society and the political spectrum as disproportionate, due to the lack of safeguards present that serve to avoid a party to be placed at a substantial disadvantage vis-à-vis the other party.

10. How do you rank the access to freedom of expression online in your country?

The case law that has been explained above reflects the current tendency in the Spanish legal system, to extend the protection of hate speech to the detriment of Freedom of Expression. This drive is also taking place in the law-making process. The emergence of bills that establish crimes of opinion can serve as evidence on the direction in which our national legislation is undertaking. Moreover, in the jurisprudence a collective approach in assessing whether expression can amount to a threat of public order are flourishing, leading to an invasion of Freedom of Expression, without taking sufficient consideration that the Internet has developed into 'one of the principal means for individuals exercising the right to Freedom of Expression and Information'.

Nevertheless, the balancing act in this new context also entails a bigger impact for other rights that clash with Freedom of Expression. As the ECtHR stated in its *Karatas v. Turkey* ruling, the higher the impact of speech, the higher its potential to disrupt public order. The internet has facilitated the engagement in hate speech. While, it is mainly politicians and the media who play a central role of fostering online hate, the internet enables a larger circle of persons to become authors of hate speech on a wide scale. As a result, despite Freedom of Expression can be regarded to be undermined, the unlimited accessibility of the internet can be used to argue for stronger protection from hate speech. Due to this free availability online, sensible online content can be accessed by vulnerable

groups, essentially minors. As a result, under certain circumstances there are certain public interests that prevail over the right to access to information, and thus they can justify a state's right to restrict certain online content in accordance with Article 10 paragraph 2 of the ECHR, as the Court ruled in *Mouvement Raëlien Suisse v. Switzerland*. The Spanish legal system has proved to be effective in the protection of the public interests of the rights of the child and other rights that prevail over freedom of expression.

Nevertheless, certain flaws can also be found. The Special Rapporteur Frank La Rue in his 2012 report especially criticised 'flawed national security and anti-terrorism laws and policies, demagogic statements by opportunistic politicians and irresponsible reporting by the mass media'. These factors have contributed to the increasing criminalisation of expressions. This phenomenon raises the question of the proportionality and the sufficiency of criminalisation for the objective of fostering tolerance and *Gemeinschaft* in society.

In the quest to fight hate speech and adopt either legal or non-legal measures, certain expressions can be considered as expressions that do not give rise to criminal or civil sanctions, but still raise concerns in terms of tolerance, civility and respect for others. The State has an important role to play in awareness raising and and should, rather than criminalise such expressions, address the underlying causes of discrimination in their society. Nevertheless, there are sectors of society that deem the criminalisation of these expressions as essential for the deterrence or dissuading effect over denigrating and discriminatory behaviours. There is yet a big difficulty on distinguishing offending, disturbing and shaking content and an incitement to discrimination, violence and racism online, as there is a fine line between them. Only those opinions that go beyond offending, shocking or disturbing and, as the ECtHR noted in Erbakan, 'spread, incite, promote or justify hatred based on intolerance' can be punished in democratic societies. Nevertheless, on the application of the Spanish Criminal Code this parameter seems to be applied in a broad way. Due to the role of Freedom of Expression on the internet and its importance in a democratic society, hate speech should be interpreted in a more restrictive way, while also taking into account the impact it may have its publishing on the web. In light of the above, we rank the access to Freedom of Expression in Spain with a 2.5 out of 5.

11. How do you overall assess the legal situation in your country regarding internet censorship?

In the assessment of internet censorship both procedural and substantial aspects will be taken into consideration in order to evaluate whether the necessary safeguard have been put in place and the sufficient protection has been granted.

In terms of the Notice and Takedown procedure, as it has been explained above a court order is needed for the adoption of the measures necessary for the blocking, filtering and taking down of online content. The need of this order answers the need of guaranteeing due process aspects in this process, by imposing the prerequisite of the ratification by a court of law that can assess whether the material and formal elements of the lawsuit have been fulfilled. While in other jurisdictions, the legislation balances the competing interests at stake ex ante and provides for a take-down or removal order in case a specific interest is violated (harm test), under the Spanish jurisdiction, the balancing of interests is left to the courts and administrative organs in specific cases, so as to prevent arbitrariness and abuse by private parties.

The model followed by Spain must be classified in order to properly assess the convenience of this proceedings. Spain does have a specific legislation on the issue of blocking, filtering and takedown of illegal internet content. The Information Society Service and E-commerce Act laid down generic legal bases and procedural aspects for the blocking and takedown procedure. Nevertheless, there are certain aspects which are regulated by the general legislation, more specifically liability and the competent organ, whether it be of administrative or judicial authority, which has jurisdiction to take appropriate action. The openness of these legal bases creates the necessity of applying other legal provisions outside of the specific legislation on this procedure, so as to develop the grounds of blocking and taking down content. It is thus making a remission outside of the said framework of the LSSI. As a result, it can be considered as a mixed system, in which a specific legal framework has been established in which blocking, filtering and take down measures are executed (LSSI), but substantial aspects of the procedure are regulated by the general legislation, creating a big complexity and a dependence on other areas of law (administrative, criminal and civil branches) for the blocking, filtering and taking down of online content. A legislative system has been put in place by the state with a view to defining the conditions and the procedures to be respected by those who engage in the blocking, filtering or takedown of online material. The legislator has not refrained from introducing a targeted legislative framework for regulating measures which enable the blocking, filtering and takedown of internet content,

but this legislation has proved to be insufficient, due to the complexity that entails the lack of homogeneity. Out of this lack of preciseness, it can be inferred that the legislator has tried to find a balance between safeguarding the dignity of internet users through a set of normative rules and enabling self-regulation of service and content providers.

The self-regulation by the parties in the internet content is carried out through Codes of Conduct foreseen in the LSSI,. Moreover, the legislator actively encourages the private sector to adopt and implement codes of conduct on the internet. This approach is intended to complement or supplement the larger set of rules on the blocking and taking down of illegal content, most of them have an imperative character.

The grounds relied on for the notice and takedown procedures broadly correspond to the interests protected under Article 10(2) of the European Convention of Human Rights. Nevertheless, these grounds are not of application to Codes of Conduct voluntarily adopted by internet service providers. As a consequence, these codes of conduct raise important issues in relation to due process, and their compatibility with Article 10 of the ECHR is highly problematic. In the absence of express and imperative legal bases for the voluntary removal and blocking of internet content, the requirements for the erasure of content or the blocking of access to URLs under the exercise of the party autonomy have been established in the case law of the courts. As the OSCE reports points out, for the effective exercise of Freedom of Expression, the action of the State ought not be limited to a duty of non-interference, but may require positive action to protect this fundamental freedom. Therefore, the State, in order to avoid the risk of illegitimate interference with fundamental rights should not depend exclusively on voluntary agreements. As our legal system is not a common law system, but rather civil or continental law the extension of self-regulation in this field does not adapt to our legal tradition. As a consequence, in our continental legal system, it is necessary for the legislator to undertake positive action in the removal of content of website operators and blocking of access by ISP, as the courts of law do not count with the sufficient margin in the event of lack of regulation. Nevertheless, in this positive action, in order to find a balance between the Right to Access of Information and the grounds of blocking and takedown, the legislator must avoid an excessive liability on internet service and access providers, so as to avoid over-removal. Moreover, the concerns in terms of information asymmetry and abuse of dominance of big technological companies fuels a big debate on the social and economic aspects that the concentration on the control of big flows of data can have on our society.

Intermediaries play an increased role as gatekeepers of the Internet-based information flows and communication networks, as they control the spaces in which individuals access and share information online and express their opinion. The public debate is gradually being taken over by private internet intermediaries, and thus the considerable influence they have will have a direct effect over governance and social *bien-être*. The mere regulation of the terms of services by the party autonomy of these intermediaries may be insufficient when public interests are at stake. Due to this increased role, the liability of the ISP that manage social networks which will become the public spaces of the future, need to be reconsidered. With the advances in ICT technologies and their extension of their usage to an ever increasing number of sectors and people worldwide, the very nature of this privately owned communicative space will change. As a result, the current limitation of responsibility of intermediaries to an effective knowledge of the online content, shows the inability of the legislator to keep up with the pace of technological developments and the role that this technology has on society.

An example of how the Spanish legislator has been able to tackle the challenges of protecting the rights of individuals in cyberspace is the specific procedure for the infringement of IP Rights on the web. For that infringement, the administrative authority of the Intellectual Property Mediation and Arbitration Commission has been given specific powers to order the blocking of unlawful content to internet service providers, whose non-compliance can lead to blocking and taking down measure with the due judicial authority. The prior need of a judicial authorisation constitutes a fundamental safeguard for the right to access of information and one of the biggest virtues of this process. After the relevant administrative authority has obtained the subsequent judicial approval of their order, interested parties are given the opportunity to challenge blocking actions through administrative procedure laws. This process has been a response of the legislator to the specificity of IP rights and the need of channels that protect these rights in cyberspace. It is a guarantee-based and specialised proceeding that sets an example for the adjudication of disputes that concern erasure and blocking of harmful online content.

Nevertheless, the Royal Decree 14/2019, adopted last year does not clearly define the powers granted to the Central Government when withdrawing physical and electrical access to the internet. As the Recommendation CM/Rec(2018)2 of the Committee of Ministers 'Any legislation should clearly define the powers granted to public authorities as they relate to internet intermediaries, particularly when exercised by law-enforcement authorities. Such legislation should indicate the scope of discretion to protect against arbitrary

application.' In the said legislation, the scope of discretion has not been sufficiently determined as it has been explained in question 9.

Table of legislation

Criminal law provisions

Provision in Spanish language	**Corresponding translation in English**
Articulo 498 Codigo Penal Los que emplearen fuerza, violencia, intimidación o amenaza grave para impedir a un miembro del Congreso de los Diputados, del Senado o de una Asamblea Legislativa de Comunidad Autónoma asistir a sus reuniones, o, por los mismos medios, coartaren la libre manifestación de sus opiniones o la emisión de su voto, serán castigados con la pena de prisión de tres a cinco años	Article 489 Criminal Code Those who use force, violence, minor or serious intimidation of prevent a member of the Congress of Deputies, the Senate or of a Legislative Assembly of an Autonomous Community from attending its meetings, or by the same means limits free expression of his opinions or casting a his vote, shall be punished with a sentence of imprisonment of three to five years
Artículo 189.8 Código Penal: Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español. Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal.	Article 189(8) Criminal Code The judges and courts will order the adoption of the necessary measures for the withdrawal of the web pages or Internet applications that contain or disseminate child pornography or in whose preparation people with disabilities in need of special protection have been used or, if appropriate, to block access to them for Internet users who are in Spanish territory. These measures may be agreed upon as a precautionary measure at the request of the Public Prosecutor.
Artículo 270.3 Criminal Code. En estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual. Excepcionalmente, cuando exista reiteración de las conductas y cuando resulte una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente.	Article 270(3) Criminal Code In such cases, the judge or court shall order the withdrawal of the works or services that are the subject of the infringement. Where, through an Internet access portal or information society service, the contents that are the subject of the intellectual property referred to in the foregoing paragraphs are disseminated exclusively or predominantly, an order shall be given for the interruption of the provision thereof, and the judge may agree to any precautionary measure having as its object the protection of intellectual property rights. Exceptionally, when there is a repetition of the conduct and when it is a proportionate, efficient and effective measure, the blocking of the corresponding access may be ordered.

Artículo 510.6 Código Penal: El juez o tribunal acordará la destrucción, borrado o inutilización de los libros, archivos, documentos, artículos y cualquier clase de soporte objeto del delito a que se refieren los apartados anteriores o por medio de los cuales se hubiera cometido. Cuando el delito se hubiera cometido a través de tecnologías de la información y la comunicación, se acordará la retirada de los contenidos. En los casos en los que, a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos a que se refiere el apartado anterior, se ordenará el bloqueo del acceso o la interrupción de la prestación del mismo.	Article 510(6) Criminal Code: The judge or court shall agree to the destruction, erasure or disabling of the books, archives, documents, articles and any kind of support that are the object of the crime referred to in the preceding paragraphs or by means of which it was committed. When the offence has been committed through information and communication technologies, it shall be agreed to remove the contents. In the cases in which, through an Internet access portal or information society service, the contents referred to in the previous section are exclusively or predominantly disseminated, the blocking of access or the interruption of the provision of the same shall be ordered.

Civil and Constitutional Law provisions

Provision in Spanish language	**Corresponding translation in English**
Article 8 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (LSSI) Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario. 1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes: a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional. b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores. c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y d) La protección de la juventud y de la infancia. e) La salvaguarda de los derechos de propiedad intelectual. En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados. En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la	Article 8 Law of services of the information society and electronic commerce. (LSSI) Restrictions on the provision of services and intra-community cooperation procedure. 1. In the event that a particular service of the information society violates or attempts to violate the principles set forth below, the competent bodies for their protection, in the exercise of the functions legally attributed to them, may take the necessary measures so that its provision is interrupted or to withdraw the data that violates them. The principles referred to in this section are the following: a) The safeguard of public order, criminal investigation, public security and national defense. b) The protection of public health or of natural or legal persons that have the status of consumers or users, even when acting as investors. c) Respect for the dignity of the person and the principle of non-discrimination based on race, sex, religion, opinion, nationality, disability or any other personal or social circumstance, and d) The protection of youth and children. e) The safeguarding of intellectual property rights. In the adoption and compliance with the restriction measures referred to in this section, the guarantees, norms and procedures provided for in the legal system to protect the rights to personal and family privacy, to the protection of data shall be respected. personal, freedom of expression or freedom of information, when they could be affected. In all cases in which the Constitution and the laws regulating the respective rights and freedoms so provide for it in an exclusive manner, only the competent judicial authority may adopt the measures provided for in this Article, as guarantor of the right to freedom of expression , of the right of literary, artistic, scientific and technical

autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información (…).	production and creation, the freedom of professorship and the right to information.
Articulo 11LSSI 1. Cuando un órgano competente hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados prestadores que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente. 2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, el órgano competente estimara necesario impedir el acceso desde España a los mismos, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España, dicho órgano podrá ordenar a los citados prestadores de servicios de intermediación que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente. 3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la	Article 11 LSSI. When a competent body had ordered, in the exercise of the powers that are legally attributed to it, that the provision of a service of the information society or the withdrawal of certain content from providers established in Spain be interrupted, and to do so necessary the collaboration of the intermediation service providers, said body may order the aforementioned providers to suspend the corresponding intermediation service used for the provision of the service of the information society or of the contents whose interruption or withdrawal have been ordered respectively . If in order to guarantee the effectiveness of the resolution that agrees to the interruption of the provision of a service or the removal of content from a provider established in a State not belonging to the European Union or the European Economic Area, the competent body deems necessary prevent access from Spain to them, and for this the collaboration of the intermediation service providers established in Spain would be necessary, said body may order said intermediation service providers to suspend the corresponding intermediation service used for the provision of the information society or content service whose interruption or withdrawal has been ordered respectively. In the adoption and compliance with the measures referred to in the preceding sections, the guarantees, norms and procedures provided for in the legal system to protect the rights to personal and family privacy, to protection shall be respected in all cases. of personal data, freedom of expression or freedom of information, when they could be affected.

libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.	
Article 13 LSSI. **Responsabilidad de los prestadores de los servicios de la sociedad de la información.** 1. Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley. 2. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes.	Article 13 LSSI. **Responsibility of the providers of the information society services.** 1. The service providers of the information society are subject to the civil, criminal and administrative liability established in general in the legal system, without prejudice to the provisions of this Law. 2. To determine the responsibility of service providers for the exercise of intermediation activities, the provisions of the following Articles shall be followed.
Article 14 LSSI. 1. Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos. No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión. 2. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.	Article 14 LSSI. 1. The operators of telecommunications networks and providers of access to a telecommunications network that provide an intermediation service that consists of transmitting through a telecommunications network data provided by the recipient of the service or providing access to it will not be responsible for the transmitted information, unless they themselves have originated the transmission, modified the data or selected these or the recipients of said data. 1. Modification shall not be understood as the strictly technical manipulation of the files that host the data, which takes place during its transmission. 2. 2. The activities of transmission and provision of access referred to in the previous section include automatic, provisional and transitory storage of the data, provided that it serves exclusively to allow its transmission over the telecommunications network and its duration does not exceed reasonably necessary time for it.
Article 15 LSSI. **Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.** Los prestadores de un servicio de intermediación que transmitan por una red	Article 15 LSSI. **Responsibility of service providers who make a temporary copy of the data requested by users.** The providers of an intermediation service that transmit over a telecommunications network data provided by a recipient of the

de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si: a) No modifican la información. b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita. c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información. d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de: 1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente. 2.º Que se ha imposibilitado el acceso a ella, o 3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.	service and, with the sole purpose of making its subsequent transmission more effective to other recipients who request them, store them in their systems automatically, provisional and temporary, they will not be responsible for the content of these data or for their temporary reproduction, if: a) They do not modify the information. b) They allow access to it only to recipients who meet the conditions imposed for this purpose, by the recipient whose information is requested. c) They respect the norms generally accepted and applied by the sector for the update of the information. d) They do not interfere in the lawful use of technology generally accepted and used by the sector, in order to obtain data on the use of the information, and e) They withdraw the information they have stored or make it impossible to access it, as soon as they have effective knowledge of: 1. That it has been removed from the place of the network in which it was initially. 2. That access to it has been disabled, or 3. That a court or competent administrative body has ordered to withdraw it or prevent it from being accessed.
Article 16 LSSI. **Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.** 1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos. Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los	Article 16 LSSI. **Responsibility of hosting or data storage service providers.** 1. The providers of an intermediation service consisting of hosting data provided by the recipient of this service will not be responsible for the information stored at the request of the recipient, provided that: a) They have no effective knowledge that the activity or information stored is unlawful or that it damages property or rights of a third party that may be indemnified, or b) If they have it, act diligently to remove the data or make access to them impossible. It will be understood that the service provider has the effective knowledge referred to in paragraph a) when a competent body has declared the illegality of the data, ordered its withdrawal or that access to it is impossible, or the existence

datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse. 2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador.	had been declared of the injury, and the provider knew the corresponding resolution, without prejudice to the procedures for detecting and removing content that the providers apply under voluntary agreements and other means of effective knowledge that could be established. 2. The disclaimer set forth in section 1 shall not operate in the event that the recipient of the service acts under the direction, authority or control of its provider.
Article 17 LSSI. **Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.** 1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente. Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse. 2. La exención de responsabilidad establecida en el apartado 1 no operará en el	Article 17 LLSI. Article 17 LSSI. **Responsibility of service providers that provide links to content or search tools.** 1. The service providers of the information society that provide links to other content or include in their directories or content search instruments will not be responsible for the information to which they direct the recipients of their services, provided that: a) They have no effective knowledge that the activity or information to which they refer or recommend is unlawful or that it damages property or rights of a third party that may be indemnified, or b) If they do, act diligently to remove or disable the corresponding link. It will be understood that the service provider has the effective knowledge referred to in paragraph a) when a competent body has declared the illegality of the data, ordered its withdrawal or that access to it is impossible, or the existence had been declared of the injury, and the provider knew the corresponding resolution, without prejudice to the procedures for detecting and removing content that the providers apply under voluntary agreements and other means of effective knowledge that could be established. 2. The disclaimer set forth in section 1 shall not operate in the event that the content provider to which it is linked or whose location is provided acts under the direction, authority or control of the

supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.	provider that facilitates the location of those contents.
Articulo 18 LSSI 1. Las administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional. Los códigos de conducta que afecten a los consumidores y usuarios estarán sujetos, además, al capítulo V de la Ley 3/1991, de 10 de enero, de competencia desleal. Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información. 2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses. Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias. Los poderes públicos estimularán, en particular, el establecimiento de criterios	Article 18 LSSI. 1. Public administrations will promote, through coordination and advice, the development and application of voluntary codes of conduct, by corporations, associations or commercial, professional and consumer organisations, in the matters regulated in this Law. The General State Administration will encourage, in particular, the development of codes of conduct at a community or international level. The codes of conduct that affect consumers and users will also be subject to chapter V of Law 3/1991, of the 10th of January, on unfair competition. The codes of conduct may, in particular, deal with the procedures for the detection and withdrawal of illegal content and the protection of the recipients against the The codes of conduct may, in particular, deal with the procedures for the detection and withdrawal of illegal content and the protection of the recipients against the electronic sending of unsolicited commercial communications, as well as the extrajudicial procedures for the resolution of conflicts arising from the provision of information society services. 2. In the elaboration of such codes, the participation of consumer and user associations and the representative organisations of persons with physical or mental disabilities shall be guaranteed, when it affects their respective interests. When its content may affect them, the codes of conduct will especially take into account the protection of minors and human dignity, and specific codes on these matters may be developed, if necessary.

comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos. 3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión.	3. The codes of conduct referred to in the preceding sections must be accessible electronically. Their translation into other official languages, in the State and of the European Union, will be promoted in order to give them greater dissemination.
Article 1902 Código Civil. El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.	Article 1902 Civil Code. The one who by action or omission causes harm to another, intervening fault or negligence, is obliged to repair the damage caused.
Articulo 138 LPI El titular de los derechos reconocidos en esta ley, sin perjuicio de otras acciones que le correspondan, podrá instar el cese de la actividad ilícita del infractor y exigir la indemnización de los daños materiales y morales causados, en los términos previstos en los artículos 139 y 140. También podrá instar la publicación o difusión, total o parcial, de la resolución judicial o arbitral en medios de comunicación a costa del infractor. Tendrá también la consideración de responsable de la infracción quien induzca a sabiendas la conducta infractora; quien coopere con la misma, conociendo la conducta infractora o contando con indicios razonables para conocerla; y quien, teniendo un interés económico directo en los resultados de la conducta infractora, cuente con una capacidad de control sobre la conducta del infractor. Lo anterior no afecta a las limitaciones de responsabilidad específicas establecidas en los artículos 14 a 17 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), en la medida en que se cumplan los requisitos legales establecidos en dicha ley para su aplicación.	**Article 138. Urgent precautionary actions and measures.** The holder of the rights recognised in this law, without prejudice to other actions that correspond to him, may request the cessation of the illegal activity of the offender and demand compensation for the material and moral damages caused, in the terms provided in Articles 139 and 140. You may also request the publication or dissemination, in whole or in part, of the judicial or arbitral decision in the media at the expense of the offender. The person responsible for the infraction will also be considered to be the one who knowingly induces the offending conduct; who cooperates with it, knowing the offending behavior or having reasonable evidence to know it; and who, having a direct economic interest in the results of the offending conduct, can control the conduct of the offender. The foregoing does not affect the specific limitations of liability established in Articles 14 to 17 of Law 34/2002, of the 11th of July, on services of the information society and electronic commerce, to the extent that the legal requirements established in said law for its application. Likewise, it may request prior adoption of the precautionary urgent protection measures regulated in Article 141. Both the specific cessation measures referred to in Article 139.1.h) and the precautionary measures provided for in Article 141.6 may also be requested, when

	appropriate, against the intermediaries whose services a third party uses to infringe intellectual property rights recognised in this law, although the acts of said intermediaries do not constitute in themselves an infraction, without prejudice to the provisions of Law 34/2002, of the 11th of July, on services of the information society and electronic commerce. Such measures must be objective, proportionate and non-discriminatory.
Articulo 139 LPI 1. El cese de la actividad ilícita podrá comprender: h) La suspensión de los servicios prestados por intermediarios a terceros que se valgan de ellos para infringir derechos de propiedad intelectual, sin perjuicio de lo dispuesto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico	Article 139 Intellectual Property Act: 1. The cease of the unlawful activity can imply: h) the discontinuation of the services offered by intermediaries to third parties that make use of such services in order to breach intellectual property rights, without prejudice to that which is foreseen in the Information Society Services and E-commerce Act.
Articulo 195 LPI 1. La Sección Segunda de la Comisión de Propiedad Intelectual ejercerá las funciones de salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los responsables de servicios de la sociedad de información a través de un procedimiento cuyo objeto será el restablecimiento de la legalidad. 2. El procedimiento de restablecimiento de la legalidad se dirigirá contra: a) Los prestadores de servicios de la sociedad de la información que vulneren derechos de propiedad intelectual, atendiendo la Sección Segunda para acordar o no el inicio del procedimiento a su nivel de audiencia en España, y al número de obras y prestaciones protegidas indiciariamente no autorizadas a las que es posible acceder a través del servicio o a su modelo de negocio. b) Los prestadores de servicios de la sociedad de la información que vulneren derechos de propiedad intelectual de la forma referida en el párrafo anterior, facilitando la descripción o la localización de obras y prestaciones que indiciariamente se ofrezcan sin autorización, desarrollando a tal	Article 195: Intellectual Property Act: 1. The second section of the Commission of Intellectual Property shall exercise all functions to safeguard intellectual property rights against possible infringements committed by services provided by Information Society through processes whose objectives are the reestablishment of lawfulness. 2.The process of reestablishing lawfulness is directed towards: a) Providers of information within Information Society that infringe intellectual property rights according to section two, to agree on the start of the legal proceedings before a Court in Spain, and to the number of works and unprotected benefits possible to access through a service or a business model. b) Information society service providers who breach intellectual property rights in the above mentioned forms, who facilitate descriptions or localise works offered without authorisation, carrying out an active, non-neutral labour, and whose activities are not limited to mere technical intermediation. Particularly, those who offer

efecto una labor activa y no neutral, y que no se limiten a actividades de mera intermediación técnica. En particular, se incluirá a quienes ofrezcan listados ordenados y clasificados de enlaces a las obras y prestaciones referidas anteriormente, con independencia de que dichos enlaces puedan ser proporcionados inicialmente por los destinatarios del servicio.	classified lists of links to such works referred to above will be considered, regardless of whether such links are provided initially by the recipients of such services.
3. El procedimiento se iniciará de oficio, previa denuncia del titular de los derechos de propiedad intelectual que se consideren vulnerados o de la persona que tuviera encomendado su ejercicio, debiendo éste aportar junto a la misma una prueba razonable del previo intento de requerimiento de retirada infructuoso al servicio de la sociedad de la información presuntamente infractor solicitando la retirada de los contenidos específicos ofrecidos sin autorización, siendo suficiente dirigir dicho requerimiento a la dirección electrónica que el prestador facilite al público a efectos de comunicarse con el mismo. Este requerimiento previo podrá considerarse cuando proceda, a efectos de la generación del conocimiento efectivo en los términos establecidos en los artículos 16 y 17 de la Ley 34/2002, de 11 de julio, siempre y cuando identifique exactamente la obra o prestación, al titular de los derechos correspondientes y, al menos, una ubicación donde la obra o prestación es ofrecida en el servicio de la sociedad de la información. En caso de que el prestador de servicios no facilite una dirección electrónica válida para la comunicación con el mismo no será exigible el intento de requerimiento previsto en este párrafo. El intento de requerimiento se considerará infructuoso si el prestador requerido no contesta o, incluso contestando, no retira o inhabilita el acceso a los contenidos correspondientes en un plazo de tres días desde la remisión del correspondiente requerimiento.	3. The proceedings will be initiated *ex officio* with a previous complaint by the holder of intellectual property rights considered breached, this individual being responsible for presenting reasonable proof of the attempt to breach his rights without authorisation in order to request the withdrawal of such content, being considered sufficient an authorisation sent to the holder of rights to permit the use of his information. This requirement shall be considered when in accordance with Articles 16 and 17 of the Law of the 11th of July, 34/2002. In the case that the service provider should not facilitate a valid address to communicate with the holder of rights, the previous statement shall not be required. The requirement shall be deemed unsuccessful when the provider does not reply, or when replying, does not remove or disable the content within a three day time frame.
4. La Sección Segunda podrá adoptar las medidas para que se interrumpa la prestación de un servicio de la sociedad de la información que vulnere derechos de propiedad intelectual o para retirar los	4. The second section can adopt measures to interrupt the provision of services when these infringe intellectual property rights, or to withdraw contents where the provider provoked or may provoke damages to

contenidos que vulneren los citados derechos siempre que el prestador haya causado o sea susceptible de causar un daño patrimonial. Dichas medidas podrán comprender medidas técnicas y deberes de diligencia específicos exigibles al prestador infractor que tengan por objeto asegurar la cesación de la vulneración y evitar la reanudación de la misma. La Sección Segunda podrá extender las medidas de retirada o interrupción a otras obras o prestaciones protegidas suficientemente identificadas cuyos derechos representen las personas que participen como interesadas en el procedimiento, que correspondan a un mismo titular de derechos o que formen parte de un mismo tipo de obras o prestaciones, siempre que concurran hechos o circunstancias que revelen que las citadas obras o prestaciones son igualmente ofrecidas ilícitamente. Antes de proceder a la adopción de estas medidas, el prestador de servicios de la sociedad de la información deberá ser requerido a fin de que en un plazo no superior a las 48 horas pueda proceder a la retirada voluntaria de los contenidos declarados infractores o, en su caso, realice las alegaciones y proponga las pruebas que estime oportunas sobre la autorización de uso o la aplicabilidad de un límite al derecho de propiedad intelectual. Transcurrido el plazo anterior, en su caso, se practicará prueba en dos días y se dará traslado a los interesados para conclusiones en plazo máximo de cinco días. La Sección dictará resolución en el plazo máximo de tres días. La interrupción de la prestación del servicio o la retirada voluntaria de las obras y prestaciones no autorizadas tendrán valor de reconocimiento implícito de la referida vulneración de derechos de propiedad intelectual y pondrá fin al procedimiento. Las medidas previstas en el presente apartado se adoptarán, con carácter previo al inicio del procedimiento, cuando el titular del servicio de la sociedad de la información presuntamente infractor no cumpla con la obligación establecida en el artículo 10 de la Ley 34/2002, de 11 julio, de servicios de la sociedad de la información y de comercio electrónico. La ejecución de las medidas	property rights. Such measures may encompass techniques and diligence duties required to the provider, when their aim is to halt infringement and avoid future infringements of the same sort. The second section can extend withdrawal measures or interrupt other acts where the rights of individuals involved in the proceedings correspond with the same holder of rights or those within the group of holders if the circumstances that reveal the cited works or services are offered illicitly. Before adopting these measures, the information society service provider is required to withdraw contents that violate these rights within no longer that 48 hours, or submit evidence proving the authorised use of the intellectual property in question. After the deadline, proposals shall be issued within two days, and the parties involved will receive an additional five days to formulate their concluding arguments. The section shall determine the verdict within three additional days. The interruption in the provision of a service or the voluntary withdrawal of non-authorised works shall receive implicit recognition referring to the infringement of intellectual property rights and shall end the proceedings. The planned measures in this Article shall be adopted prior to the start of the proceedings when the presumed breacher is the information society service provider and does not comply with Article 10 of the Law on Information Society Services and Electronic Commerce of the 11th July, 34/2002. The execution of these measures shall be in accordance with the following paragraph.

acordadas conforme al presente párrafo se realizará conforme a lo previsto en el apartado siguiente. 5. En caso de falta de retirada voluntaria y a efectos de garantizar la efectividad de la resolución dictada, la Sección Segunda podrá requerir la colaboración necesaria de los prestadores de servicios de intermediación, de los servicios de pagos electrónicos y de publicidad, requiriéndoles para que suspendan el correspondiente servicio que faciliten al prestador infractor. En la adopción de las medidas de colaboración la Sección Segunda valorará la posible efectividad de aquellas dirigidas a bloquear la financiación del prestador de servicios de la sociedad de la información declarado infractor. El bloqueo del servicio de la sociedad de la información por parte de los proveedores de acceso de Internet deberá motivarse adecuadamente en consideración a su proporcionalidad, teniendo en cuenta la posible eficacia de las demás medidas al alcance. En el caso de prestarse el servicio utilizando un nombre de dominio bajo el código de país correspondiente a España (.es) u otro dominio de primer nivel cuyo registro esté establecido en España, la Sección Segunda notificará los hechos a la autoridad de registro a efectos de que cancele el nombre de dominio, que no podrá ser asignado nuevamente en un periodo de, al menos, seis meses. La falta de colaboración por los prestadores de servicios de intermediación, los servicios de pagos electrónicos o de publicidad se considerará como infracción de lo dispuesto en el artículo 11 de la Ley 34/2002, de 11 de julio. En todo caso, la ejecución de la medida de colaboración dirigida al prestador de servicios de intermediación correspondiente, ante el incumplimiento del requerimiento de retirada o interrupción, emitido conforme al apartado anterior, por parte del prestador de servicios de la sociedad de la información responsable de la vulneración, exigirá la previa autorización judicial, de acuerdo con el procedimiento regulado en el apartado segundo del artículo 122 bis de la Ley	5. In the case that information is not voluntarily withdrawn, in order to guarantee the effectiveness of this Resolution, section two may require the collaboration of intermediary service providers, electronic payment service providers, and publicity providers, to suspend the service where a breach is identified. When adopting collaboration measures, the second section shall value the possible effectiveness of those measures aimed at blocking the financing of the information society service provider declared offender. The blocking of an information society service by internet providers must be proved proportional in its outreach. In the case that the service utilises a Spanish internet domain (.es) or any other domain registered in Spanish territory, the second section shall notify the acts to the corresponding registration authority to cancel the domain, which cannot be reassigned within a period of six months. The lack of collaboration on behalf of information society service providers, electronic payment service providers or publicity providers shall be considered as a breach of the Law of the 11th July, 34/2002. In any case, the execution of collaboration measures destined to intermediary service providers, if there is an infringement in the withdrawal of the information stated in the previous paragraph, on behalf of the information society service provider, it will be demanded that he comply with Article 2 of the Law on Contentious-Administrative Proceedings of the 13th of July, 29/1998.

29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. 6. El incumplimiento de requerimientos de retirada de contenidos declarados infractores, que resulten de resoluciones finales adoptadas conforme a lo previsto en el apartado 4 anterior, por parte de un mismo prestador de servicios de la sociedad de la información de los descritos en el apartado 2 anterior, constituirá, desde la segunda vez que dicho incumplimiento tenga lugar, inclusive, una infracción administrativa muy grave sancionada con multa de entre 150.001 hasta 600.000 euros. La reanudación por dos o más veces de actividades ilícitas por parte de un mismo prestador de servicios de la sociedad de la información también se considerará incumplimiento reiterado a los efectos de este apartado. Se entenderá por reanudación de la actividad ilícita el hecho de que el mismo responsable contra el que se inició el procedimiento explote de nuevo obras o prestaciones del mismo titular, aunque no se trate exactamente de las que empleara en la primera ocasión, previa a la retirada voluntaria de los contenidos. Incurrirán en estas infracciones los prestadores que, aun utilizando personas físicas o jurídicas interpuestas, reanuden la actividad infractora.	6. The breaching of requirements regarding the withdrawal of infringing content, resulting in resolutions adopted according to paragraphs 2 and 4, shall impose, if a reiterated breaching has taken place, a fine betreen 150,000€ and 600.000€. Reiterated infringement is understood as the infringement in two or more occasions of the law by the same information society service provider. Any natural person or legal entity can be subject to fine.
Artículo 1 *Ley reguladora de la cláusula de Conciencia de Profesionales de la Información*: La cláusula de conciencia es un derecho constitucional de los profesionales de la información que tiene por objeto garantizar la independencia en el desempeño de su función profesional	Article 1 of the *Law regulating the Conscience Clause of Information Professionals*: The conscience clause is a constitutional rights pertaining information professionals (journalists) that has as its object the safeguard of the independence in the exercise of its profession
Articulo 2 *Ley reguladora de la Cláusula de Conciencia de Profesionales de la Información*: 1. En virtud de la cláusula de conciencia los profesionales de la información tienen derecho a solicitar la rescisión de su relación jurídica con la empresa de comunicación en que trabajen: a) Cuando en el medio de comunicación con el que estén vinculados laboralmente se produzca un cambio sustancial de orientación informativa o línea ideológica.	Article 2 of the *Law regulating the Conscience Clause of Information Professionals*: 1. Under the conscience clause, the information professionals have the right to request the termination of their legal relationship with the media company in which they work: (a) When there is a substantial change in the information orientation or ideological line in this media company.

b) Cuando la empresa les traslade a otro medio del mismo grupo que por su género o línea suponga una ruptura patente con la orientación profesional del informador. 2. El ejercicio de este derecho dará lugar a una indemnización, que no será inferior a la pactada contractualmente o, en su defecto, a la establecida por la Ley para el despido improcedente.	(b) When this media company transfers them to another medium of the same group with another line which meant a break with the professional orientation of the informant. 2. The exercise of this right will give rise to a compensation, which will not be less than the contractually-agreed or, failing this, it will be the one regulated for unfair dismissal.
Articulo 6 *Real Decreto 14/2019 de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.:* El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional. En concreto, esta facultad excepcional y transitoria de gestión directa o intervención podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional. Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el Título III de esta Ley, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y de la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de los correspondientes servicios o de la explotación de las correspondientes redes. Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias	Article 6 of *Royal Decree 14/2019 of the 31st of October, adopting urgent measures of public security in the area of digital administration, public contracting and telecommunications*: The Government may exceptionally and temporarily agree to the direct management or intervention by the National State Administration of electronic communication networks and services in exceptional circumstances when it could affect the public order, the public security and national security. Specifically, this exceptional and transitional power of direct management or intervention may affect any infrastructure, associated resource or element, network level or service required to preserve or restore public policy, public security and national security. Likewise, in the case of a breach of obligations of public service found in Title III of this Royal Decree, the Government, following a mandatory report from the National Commission for Markets and Competition and also on an exceptional and temporary basis, may agree to the direct management or intervention by the National State Administration of the relevant services or the operation of the relevant networks. The agreements related to the direct management or intervention thereof or those related to the intervention or operation of networks found in the preceding paragraphs will be adopted by the Government on its own initiative or at the request of a competent Public Administration. In this latter case, it will be necessary for the Public Administration to be competent in security or for the

en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.»	provision of public services affected by the abnormal operation of the service or of the electronic communications network. In the event that the procedure is initiated at the request of a Public Administration other than the National State Administration, the latter will be considered as interested and may issue a report prior to the final decision.
Artículo 20 Constitución española Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción. b) A la producción y creación literaria, artística, científica y técnica. c) A la libertad de cátedra. d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades. 2. El ejercicio de estos derechos no puede restringirse mediante ningún tipo de censura previa. 3. La ley regulará la organización y el control parlamentario de los medios de comunicación social dependientes del Estado o de cualquier ente público y garantizará el acceso a dichos medios de los grupos sociales y políticos significativos, respetando el pluralismo de la sociedad y de las diversas lenguas de España. 4. Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia. 5. Sólo podrá acordarse el secuestro de publicaciones, grabaciones y otros medios de información en virtud de resolución judicial.	Article 20 Spanish Constitution The following rights are recognised and protected: a) the right to freely express and spread thoughts, ideas and opinions through words, in writing or by any other means of reproduction,in second place b) the right to literary, artistic, scientific and technical production and creation, c) the right to academic freedom d)the right to freely communicate or receive truthful information by any means of dissemination. However, the law shall regulate the right to the clause of conscience and professional secrecy in the exercise of these freedoms. 2. The exercise of these rights cannot be restricted through any kind of prior censure. 3. The law will govern the organisation and parliamentary control of the means of communication that are dependent on the State or any other public entity and will guarantee the access to those means of communication to significant social and political groups, in full respect of political pluralism present in society and of the various languages in Spain. 4. These freedoms are limited by the respect for the rights recognised in Title I of said Constitution, by the legal provisions implementing it, and especially by the right to honour, privacy, personal reputation and to the protection of youth and childhood. 5. The seizure of recordings and publications and other means of information can only be carried out through a judicial order.

Bibliography

English titles

Legislation

Charter of Fundamental Rights of the European Union

Directive 95/46/EC

Information Society Services and Electronic Commerce Act. Law 34/2002 of the 11th of July

Royal Decree 1/2007 of 16th of November, whereby the General Law for the Defense of the Consumers and Users and other complementary legislation is approved.

Regulatory Law of the Contentious Administrative Jurisdiction. Law 29/1998 of the 13th of July.

Criminal Code. Organic Law 10/1995 of the 23rd of November.

Civil Code

Reports

Aronovitz, A., "Comparative study on blocking, filtering and take-down of illegal Internet content", Swiss Institute of Comparative Law, Avis 14-067, 20 December 2015

Council of Europe, 'Recommendation No. R (97) 20 of the 30th of October 1997 of the Committee of Ministers to member states on "hate speech".

Jaime Goyena Huerta, Some criminal matters on hate speech. (Aranzadi Journal on Law and Criminal Procedure no. 49/2018)

House of Lords European Union Committee. "EU Data Protection law: a 'right to be forgotten'." Second Report of Session 2014-15 (2014).

Ministry of Industry,Commerce and Tourism & RED.es, Digital Society and Law (Official Bulletin of the State, 2018)

Murray Andrew, and Murray Andrew. Information Technology Law : the Law and Society / Andrew Murray. Third edition. Oxford: Oxford University Press, 2016

Peguera, Miquel. "In the Aftermath of Google Spain : How the 'right to Be Forgotten' Is Being Shaped in Spain by Courts and the Data Protection Authority." International Journal of Law and Information Technology 23, no. 4 (December 2015): 325–347.

TAMARIT SUMALLA, J.M., "Hate speech crimes in social networks" Internat, Law and Politics Journal N.º 27 (Septiembre, 2018)

TERUEL LOZANO, G.M, "Intolerant expressions, hate crimes and freedom of expression: a difficult balance", Legal Journal Autonomous University of Madrid, No.36, 2017-II

TERUEL LOZANO, G.M, "Freedom of expression and censure on the internet", Deusto Studies, Vol. 62/2, Bilbao, July-December 2014

German M Teruel Lozano, When words generate hatred: limits to freedom of expression in the Spanish Constitutional Order (University of Murcia, 2018)

Books

Voorhoof, Dirk. (2015). The European Convention on Human Rights: The Right to Freedom of Expression and Information restricted by Duties and Responsibilities in a Democratic Society. Ḥuqūq-i Bashar. 7.

Periodicals

El Condifencial, the present and the future of responsability in the internet https://blogs.elconfidencial.com/espana/blog-fide/2019-07-04/presente-futuro-responsabilidad-internet_2100434/ Accessed 18 February 2020

Los 40, " the woman that did versions of Pablo Alboran had the obligation to erase such content"
https://los40.com/los40/2017/09/01/tecnologia/1504260082_730300.html Acessed 18 February2020

La Vanguardia, Instagram considers as graphic violence the pictures of a graphic stew and blocks them
https://www.lavanguardia.com/vida/20191022/471143662208/richard-barreira-instagram-elimina-fotos-cocido-gallego.html Accessed 20 February 2020

Europapress, Spain considers self-regulation of social netowrks insufficient to tackle disinformation https://www.europapress.es/sociedad/noticia-espana-ve-insuficiente-autorregulacion-redes-sociales-atajar-desinformacion-20190523142920.html Accessed 18 February 2020

Digital resources

Javier Álvarez Hernando, 'Material and procedural aspects of illegal content take down on the Internet' (AC Abogados, 8 June 2011), <https://bit.ly/2UF1tQu> accessed 07 February 2020

Carolina Pina and Cristina Mesa, 'EU Recommendations on take down of Internet content' (Garrigues Digital, 23 March 2018), <https://bit.ly/377XrlX> accessed 06 February 2020

Spanish Data Protection Agency, Adaptation of treatments of Data that introduce AI to GDPR , February 2020.
https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf
Accessed 22 February 2020

Case law

Case of Stern Taulats And Roura Capellera v. Spain, Judgment of ECHR (3d Section) of the 13th of March, 2018

Judgement of Supreme Court No. 4/2017 of the 18th of January

Judgment of the Constitutional Court 112/2016

Judgment of the Constitutional Court 177/2015, of the 22nd of July.

Judgment of the Constitutional Court 176/1995, of the 11th of December.

Judgement of the Constitutional Court No. 14/1985, of the 31st of January

Judgement of the Constitutional Court No. 52/1983 of the 17th of June

Judgement of the Constitutional Court 28/1982, of the 26th of May

Judgement of Supreme Court No. 4/2017 of the 18th of January, 2017

Judgement of the High National Court (Criminal Chamber, Section 1) No. 6/2018 of the 18th of September.

Judgement of the High National Court (Criminal Chamber, Section 1) No. 4/2018 of the 10th of July

Judgement of the High National Court (Criminal Chamber, Section 1) No. 3/2018 of the 2nd of March

Judgment of the Provincial Court of Barcelone (Section 10ª) Ruling no. 299/2019 of the 21st of May

Judgement of the Provincial Court of Barcelone (Section 8ª) Ruling no. 607/2018 of the 7th of December.

Judgement of the Provincial Court of the Balear Islands (Section 1ª)Ruling no. 312/2013 of the 10th of December.

Order of the Commercial Court of Barcelona, No. 195/12 of the 30th of April 2012

Case No. E/2012/00012 of the IP Commission

Spanish titles

Reports

TERUEL LOZANO, G.M, "Expresiones intolerantes, delitos de odio y libertad de expresión: un difícil equilibrio", Revista Jurídica Universidad Autónoma de Madrid, No. 36, 2017-II

TERUEL LOZANO, G.M, "Libertad de expresión y censura en internet", Estudios de Deusto, Vol. 62/2, Bilbao, Julio-Diciembre 2014, pages 60-61

Books

Miguel Peguera Poch, La exclusión de responsabilidad de los intermediarios de internet (COMARES, 2007)

Roberto Yanguas Gómez, Contratos de conexión a internet, "hosting" y búsqueda (1st. Edn, Aranzadi, 2012)

Case law

AEPD decision of the 16th of December 2014 (TD-01369-2014)

Judgement of the Constitutional Court no. 13/1985, of the 31st of January

Judgement of the Constitutional Court no. 52/1983, of the 17th June

Judgement of the Constitutional Court no. 4/2017 of 8 January.

Sentencia de la Audiencia Nacional (Sala de lo Penal, Sección 1ª) núm. 6/2018 de 18 de septiembre

Sentencia de la Audiencia Nacional (Sala de lo Penal, Sección 1ª) núm. 4/2018 de 10 de julio

Sentencia de la Audiencia Nacional (Sala de lo Penal, Sección 1ª) núm. 3/2018 de 2 de marzo

Auto del Juzgado de lo Mercantil de Barcelona núm. 195/12 de 30 de abril

Caso núm. E/2012/00012 de la Comisión de la Propiedad Intelectual

ELSA Turkey

Contributors

National Coordinator

Berin Günay

National Academic Coordinator

Elif Benan Yaman

National Researchers

Berk Hasan Özdem

Efsun Eryürek

Gözde Diktaş

İrem Arisoy

Muhammed Siraceddin Tapan

Özge Dirim Çiftçi

Sevgi Özben

Zeynep Özge Oğuz

Zülal Erdoğan

National Linguistic Editor

Ecem Kumsal Başyurt

National Academic Supervisor

Ulaş Karan

Acknowledgements

This research was supported by the European Law Student Association (ELSA). We are grateful to our national academic supervisor, who provided insight and expertise that greatly assisted the research process, although he may not agree with all of the interpretations/conclusions of this paper and any errors are entirely ours and should not diminish his reputation. We would also like to show our gratitude to the reviewers for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

Introduction

A democratic society hinges on the people being able to hold informed opinions and express them. It is important that people are able to ask questions of the people in power and find out about decisions which affect them and their fellow citizens. Therefore, this makes the Freedom of Expression an essential right for a society to be democratic.

With the development of technology all over the world today, importance of Freedom of Expression has increased. The principle of Freedom of Expression and human rights has become a must to apply not only to traditional media but also the Internet and all types of emerging media platforms, which will contribute to development, democracy and communication. However, it has also become one of the most violated human rights.

In Turkey, even though the Freedom of Expression is not regulated as an absolute right or a framework article under the Turkish Constitution; it has been regulated by international treaties and agreements and also it is mentioned and implicitly regulated through the articles of related rights under the Turkish Constitution such as Freedom of Expression and dissemination, freedom of thought and opinion, freedom of science and art, freedom of press and etc. On the other hand, Internet freedom in Turkey remained highly restricted in the past years, which was characterised by increased self-censorship, a growing list of blocked news sites, and sweeping arrests for criticising military operations. The increasingly 'security-first' outlook has not been balanced with due concern for rights and freedoms online, including privacy and Freedom of Expression. As a result, Turkish authorities have received criticism from the European Court of Human Rights, the Venice Commission, and international and domestic human rights organisations.

1. How is Freedom of Expression protected in your national legislation and which legislation is in place to protect against limitation towards Freedom of Expression?

The Freedom of Expression is one of the pillars of Turkish democracy and protected as a fundamental human right under international treaties, primarily under European Convention on Human Rights, as well as Turkish domestic legislation, its code laws and regulations, primarily under the Constitution of the Republic of Turkey ('*Constitution*') in Articles 25, 26, 27, 28 and 32.

Under the Constitution, the Freedom of Expression has not been regulated as a framework article, but rather thoroughly in terms of both the means and the way of using Freedom of Expression. Between the Articles of 25 and 32 of the Constitution, the freedom of thought and opinion (Article 25), the Freedom of Expression and dissemination of thought (Article 26), the freedom of science and art (Article 27), the freedom of the press (Article 28) and the right to rectification and response (Article 32) are regulated.

Under the Constitution, international treaties have the force of law, except in cases of disputes on fundamental rights and freedoms between international treaties and domestic legislation where they contain different provisions on the same subject, international treaties are taken into consideration. The Republic of Turkey has been a Member State of the European Convention on Human Rights ('*Convention*') since 1950 and came into force in 1954. Thus, excluding Turkey's responsibilities and obligations under the Convention in the international law level, Turkish legal system has designated a primary role to the Convention for protection of Freedom of Expression, among other rights regulated with it. It can be interpreted that just in this specific case, the Convention can be considered above domestic code laws and below the Constitution. This is one of the reasons that the Convention has a great importance for the legal protection of the right to Freedom of Expression in Turkey.

Since Freedom of Expression is not regulated as an absolute right in the Constitution and it is regulated implicitly by many articles in the Constitution that include the Freedom of Expression one way or another; the articles on limitation and restrictions on limitation must be evaluated separately.[1985] However, Article 13 of the Constitution regulates the restrictions on the limitations of fundamental rights and freedoms. So, Freedom of Expression is

[1985] Ulaş Karan, Freedom of Expression, Manuals Series for Individual Application to the Constitutional Court – 2, European Council [2018] 109.

subjected to the limitation of fundamental rights and freedoms regulated in Article 13 of the Constitution.

According to Article 13 of the Constitution, the fundamental rights and freedoms can only be restricted by law and only for the reasons set out in the relevant articles of the Constitution. The expression 'restricted by law' in Article 13 of the Constitution may create the impression that the limitation can only be applied by the legislature. However, in Article 11 of the Constitution, it is regulated that legislative, executive and judicial organs, administrative authorities and other institutions and individuals are connected by the basic legal rules of the constitutional provisions. Therefore, not only the legislature but also the executive and judicial bodies must comply with the restrictions in question.[1986] However, the limitation on the fundamental rights and freedoms should be regulated and applied in a way that they do not touch the essence of rights and freedoms. Also, the limitations cannot be against the word and spirit of the Constitution, the requirements of the democratic social order and the secular Republic, and the principle of proportionality. These criteria are in line with the criteria used by the ECtHR, and there is no obstacle for the judicial bodies to implement the examination method applied by the ECtHR.

Within the scope of Turkish legislation or Turkish legal academia, there is no agreed-upon definition on 'censor' or 'censorship'. However, the expression 'censor' has been regulated under the Constitution in Article 28 paragraph 1 by stating that 'the press is free, and shall not be censored.' Mainly, *Anayasa Mahkemesi* (Turkish Constitutional Court) has been defining which actions are considered as censorship and the expression has been usually regarded within the context of the press, whether it is published on paper or on the internet[1987].

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

2.1. Turkish adherence to international conventions in respect of Freedom of Expression

Turkey is a state party to major international human rights instruments such as the international Covenant on Civil and Political Rights (hereinafter, 'ICCPR') and the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter, 'ECHR'). Freedom of Expression is

[1986] Ibid.

[1987] *Medya Gündem Dijital Yayıncılık Ticaret A.Ş.* [2013] Constitutional Court of the Republic of Turkey 2623 [2015] para 53 [Turkish].

guaranteed by Article 10 ECHR, by Article 19 ICCPR and by Article 19 of the Universal Declaration of Human Rights.

Concerning the Turkish legislation regarding internet censorship, it should be mentioned in the first place that Article 90 of the Constitution of the Republic of Turkey constitutes an interpretation tool of utmost importance whereby it is stated that 'In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail.' This provision is noteworthy since it not only favours the application of norms of international agreements,[1988] but it also implies the necessity of an interpretation in favour of these latter.[1989] In other words, as noted by the Turkish Constitutional Court, should a domestic provision of law be in contradiction with the ECtHR jurisprudence on the interpretation of a certain ECHR Article, the case should be resolved in accordance with Article 90 of the Constitution.[1990] Such approach was illustrated in case Adalet Mehtap Buluryer, where the Turkish Constitutional Court found that overlooking ECtHR jurisprudence in Turkish Law violated the right to a fair trial of the applicant.[1991]

However, according to the findings of Council of Europe Commissioner for Human Rights during his April 2016 visit the application by Turkish courts and prosecutors of the statutory framework showed an increasingly negative trend which counterbalanced and reversed some positive efforts of the Turkish Constitutional Court to achieve a more ECHR-compliant interpretation of the Turkish legislation.[1992]

2.2. Turkish legal framework concerning internet censorship

Internet regulation in Turkey is primarily authorised under the Electronic Communications Law[1993] (hereafter 'ECL') and the Law numbered 5651, entitled

---

1988 *Sevim Akat Eşki App. no: 2013/2187,* [2013] Constitutional Court of the Republic of Turkey 41 [Turkish]; *Adalet Mehtap Buluryer App no: 2013/5447* Constitutional Court of the Republic of Turkey [2013] 46 [Turkish].

1989 Ulaş Karan, İfade Özgürlüğü: Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 2 (MRK 2018) 129 [Turkish].

1990 *Sevim Akat Eşki App. no: 2013/2187,* [2013] Constitutional Court of the Republic of Turkey 45-46 [Turkish].

1991 *Adalet Mehtap Buluryer App no: 2013/5447* Constitutional Court of the Republic of Turkey [2013] 52-53 [Turkish].

1992 *'Turkey: security trumping human rights, free expression under threat'* (Council of Europe 14. April 2016) <https://www.coe.int/en/web/commissioner/-/turkey-security-trumping-human-rights-free-expression-under-threat?inheritRedirect=true&redirect=/en/web/commissioner/country-report/turkey> accessed 20 February 2020.

1993 Law n. 5809 (Electronic Communications) 2008 [Elektronik Haberleşme Kanunu].

The Law on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts[1994] (hereafter 'Internet Law') and carried out by the Information and Communication Technologies Authority (hereafter 'ICTA').

The Internet Law enacted on 4 May 2007, *inter alia*, regulates the access restriction procedure for specific crimes, and the further details for combating such crimes, particularly in cases of emergency (Article 8 and Article 8/A) as well as the notice and take down procedures, the removal of content and blocking access to such content, where such content violates personal rights (Article 9 and 9/A).

Amendments were made to the Internet Law in 2014, through which some new procedures concerning access-blocking to websites were introduced. For instance, while there was no specific time-limit before the amendment, Article 8 currently provides that the decision to block access to a website under Article 8 may only be given for a limited period of time. The amendment introduced to Article 9(4) brought the obligation for the judge to order the blocking of a specific publication (for instance an URL) rather than of the whole website, except in the case where this is not possible due to technical reasons.

The 2014 amendments were presented by 'an omnibus bill including new regulations on Internet usage which gives more power to the country's national telecommunications authority.'[1995] Introducing alternative procedures for blocking access, this bill increased the powers of the Presidency of Telecommunication whose powers subsequently transferred to Information and Communication Technologies Authority (BTK) with its shut. For instance, the new Article 9(A), provides in its paragraph 8 that 'in circumstances where it is considered that delay may present a risk of violation of the confidentiality of private life, the denial of access shall be carried out by the Information and Communication Technologies Authority upon the direct instructions of the President of Information and Communication Technologies Authority.'[1996]

1994 Law n. 5651 (Law on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts) 2007[İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun].

1995 '*Turkey's general assembly ratifies Internet bill*' (Anadolu Agency 26 February 2014) <https://www.aa.com.tr/en/turkey/turkey-s-general-assembly-ratifies-internet-bill/179203> accessed 20 February 2020.

1996 Translation provided by: European Commission for Democracy Through Law (Venice Commission), Opinion on Law No. 5661 On Regulation of Publications on the Internet and Combating Crimes Committed by Means of such Publication ('The Internet Law') (Opinion No. 805 / 2015, CDL-AD(2016)011) (Council of Europe 2016).

With the amendments introduced in 2014 to Articles 4(3) and 5(5), the content provider and the hosting provider became obliged 'to furnish the Presidency with such information as it may demand within the scope of the performance by the Presidency of functions delegated to it by this Law and other legislation, and shall take such measures as may be directed by the Presidency'.[1997] These provisions were subsequently found unconstitutional by the Constitutional Court of the Republic of Turkey by its judgment dated 8 December 2015 which entered into force on 28 January 2017.

The Internet Law was amended again in March 2015. A new Article 8(A) was introduced, which provided for another access-blocking procedure with the title 'Removal of content and/or blocking of access in circumstances where delay would entail risk'. The procedure started at the initiative of the President of the Information and Communication Technologies Authority and the Ministry concerned with the protection of national security and public order for a number of reasons, such as the protection of national security or public order. The blocking measure has become subject to ex post judicial control process by the introduction of Article 8(A)(2).

Currently, four different access-blocking procedures are active according the Internet Law, namely (1) Article 8 entitled ('The decision to deny access, and implementation thereof'); (2) Article 8A entitled ('Removal of content and/or blocking of access in circumstances where delay would entail risk'); Article 9 entitled ('Removal of content from publication, and blocking of access'); and Article 9A entitled ('Blocking access to content on grounds of the confidentiality of private life').

Under Article 8, a decision on access-blocking shall be issued should there are sufficient grounds for suspicion that the content constitutes any of the following crimes: (1) Incitement to commit suicide (Article 84 of the Criminal Code), (2) Sexual exploitation of children (Article 103, first paragraph), 3) Facilitating the use of narcotic or stimulant substances (Article 190), (4) Supply of substances which are dangerous to health (Article 194), (5) Obscenity (Article 226), (6) Prostitution (Article 227), (7) Providing premises or facilities for gambling (Article 228), and any of the offences under the Law on Offences against Atatürk (the founding father of the Republic of Turkey), Statute 5816, dated 25 July 1951.

[1997] Translation provided by: European Commission for Democracy Through Law (Venice Commission), Opinion on Law No. 5661 On Regulation of Publications on the Internet and Combating Crimes Committed by Means of such Publication ('The Internet Law') (Opinion No. 805 / 2015, CDL-AD(2016)011) (Council of Europe 2016).

The procedure on access-blocking under Article 8A concerns the protection of the right to life, security of life and property, national security, public order and public health as well as the prevention of commission of crimes.

Article 9 provides for a procedure for access-blocking/removal of content in cases where information published online results in the violation of personal rights. According to Article 9(1), asserting that their personal rights have been violated, real persons, legal entities, institutions and organisations may apply for the removal of publication by means of a warning to the content provider or, should the content provider cannot be contacted, to the hosting provider. These latter may also demand denial of access to the publication by appealing directly to a judge who shall make a decision within 24 hours without holding a hearing.

According to the procedure provided for in Article 9A, persons who assert that the confidentiality of their private life has been breached by an online publication may request access-blocking by applying directly to the Information and Communication Technologies Authority.

There is a 'fundamental difference' between the procedure foreseen under Article 8 of the Law, and those implemented by Articles 8A, 9 and 9A explained by the European Commission for Democracy Through Law (Venice Commission).[1998] Under Article 8, the measure of access-blocking appears as a 'precautionary measure' or 'interlocutory measure', taken in the framework of criminal proceedings related to the crimes listed under Article 8(1) a) and b), by a judge at the investigation stage and by a court at the prosecution stage, or by a public prosecutor at the investigation stage where delay would present a risk. This 'precautionary measure' is dependent on the substantial criminal procedure. On the other hand, Articles 8A, 9 and 9A establish autonomous access-blocking procedures that are not contingent on any other substantive criminal or civil procedure. Put differently, access-blocking decisions taken in the context of Articles 8A, 9 and 9A are not 'precautionary measures'.

In addition to procedures foreseen in the Internet Law, in 2018, the Turkish parliament passed a law authorising the national broadcast media regulator, the High Council for Broadcasting (RTÜK) to monitor and regulate internet services. Under the law, online video and streaming services are required to apply for a license to broadcast to Turkish internet users.[1999]

[1998] Translation provided by: European Commission for Democracy Through Law (Venice Commission), Opinion on Law No. 5661 On Regulation of Publications on the Internet and Combating Crimes Committed by Means of such Publication ('The Internet Law') (Opinion No. 805 / 2015, CDL-AD(2016)011) (Council of Europe 2016) para 33.

[1999] *'Turkey's Government Takes New Powers to Censor the Internet'* (Economist 24 May 2018)

Furthermore, there are secondary regulations such as ordinances enacted based on the internet law, namely, ordinance on the procedures about granting business certificates for the host provider and access provider, ordinance on the procedures for regulating the content of online publications. Secondary regulations elaborate upon the provisions of the IA.

2.3. Case Law of the European Court of Human Rights

In its first ruling addressing access-blocking measures on the internet taken on the basis of Turkish Internet Law, *Ahmet Yıldırım v. Turkey*,[2000] the ECtHR has ruled that blanket website blocking violated the right to Freedom of Expression under the ECHR. The case involved a court decision concerning total access-blocking to the Google Sites Platform from Turkey. In order to prevent further access to one particular website, which contained material deemed offensive to the memory of Mustafa Kemal Atatürk,[2001] violating Article 8(1)b of Internet Law, it was necessary to block the entire Google Sites platform hosting the offensive website, since it is technically not possible to block a single URL.

The ECtHR considered that neither the complainant's academic website nor the web hosting platform in general fell within the scope of said provision because the legality of their content had never been contested within a court proceeding. Furthermore, although the decision of 24 June 2009 had found Google Sites to be responsible for the site it hosted, no provision was made in the Turkish Internet Law for the wholesale blocking of access such as the one ordered by the national court.

The Commissioner for Human Rights of the Council of Europe found that, despite the clear guidance of the Court in the *Ahmet Yıldırım* v. *Turkey* judgment, the subsequent changes to the Internet Law since 2014, rather than ensuring compliance with the Convention, broadened the scope of internet censorship, and therefore concluded that the censorship of the internet and blocking of websites in Turkey continued to be '*exceptionally disproportionate*'. [2002]

The recent *Wikimedia Foundation, INC. v. Turkey*[2003] case concerned the blanket ban imposed on Wikipedia web site which is a free online encyclopaedia. On 28 April 2017 the ICTA requested that five URL addresses be removed from the Wikipedia website and the following day access to the entire web site was

<https://www.economist.com/europe/2018/05/24/turkeys-government-takes-new-powers-to-censor-the-internet> accessed 20 February 2020.

2000 *Ahmet Yıldırım* v. *Turkey* no 3111/10 ECHR [2012].

2001 Mustafa Kemal Atatürk is the founder of the modern Republic of Turkey.

2002 Commissioner for Human Rights of the Council of Europe, *Memorandum on Freedom of Expression and media freedom in Turkey (CommDH(2017)5)* (Council of Europe 2017) para 111.

2003 *Wikipedia Foundation, Inc. v. Turkey*, App. no. 25479/19. (lodged on 29 April 2019).

blocked by the ICTA. On the same day, this act was approved by the Ankara 1st Magistrates' Court and the applicant's objection was rejected by the same judge on 4 May 2017. Therefore, the Wikimedia Foundation as well as the academics Yaman Akdeniz and Kerem Altıparmak filed separate individual applications with the Turkish Constitutional Court. The Constitutional Court did not issue a judgment and for almost two and half years there was no development involving the individual applications lodged with the Constitutional Court. Because of the delays, in May 2019, the Wikimedia Foundation filed an application with the ECtHR, stating that the ban was '*a violation of the right to Freedom of Expression*'. The ECtHR expedited the case and gave Turkey until the end of October to present evidence that a ban on Wikipedia is in line with European human rights standards. The Constitutional Court of Turkey weighed in on the issue on 11 September 2019 to decide whether the ban is in violation of the Freedom of Expression or not. On 26 December 2019, the court ruled in a 10–6 vote that the block of Wikipedia violated the Freedom of Expression and ordered it to be lifted immediately. After the decision overruling the initial ban, Turkish authorities granted users access to Wikipedia on late 15 January 2020. The decision was officially announced in the Official Gazette on the same day.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

3.1. Is content which is unlawful in civil law and content which is illegal under criminal law treated differently?

With the Regulation of Publications on the Internet and Combining Crimes Committed by Means of Such Publication Law, Statue 5651; access-blocking has been brought to the Turkish Law system for the first time and criminal liability of internet subjects has been regulated.

The access-blocking procedure which is regulated in Article 8 of 'the Regulation of Publications on the Internet and Combining Crimes Committed by Means of Such Publication Law', constitutes any of the crimes listed below and are subject to the '*numerus clausus*' principle:

- Incitement to commit suicide (Criminal Code Article 84)
- Sexual exploitation of the children (Criminal Code Article 103/1)
- Facilitating the use of narcotic or stimulant substances (Criminal Code Article 190)

— Supply of substances which are dangerous to health (Criminal Code Article 194)
— Obscenity (Criminal Code Article 226)
— Prostitution (Criminal Code Article 227)
— Providing premises or facilities for gambling (Criminal Code Article 228)
— Any of the offences under the Law on Offences against Atatürk, Statute 5816, dated 25 July 1951

In addition, with the paragraph 14, which is added to Article 8, specifies that the institutions and organisations defined in paragraph 3 of Article 3, Paragraph 1 of the Law of Regulation of Tax, Fund and Shares from Revenue of Chance Games have been given the right to prohibit access to content containing crimes related to their own legislation.

The amendment of the Internet Law in March 2015 added a new Article 8A providing for an additional procedure for removal of content and/or blocking of access in order to protect the right to life or security of life and property, national security and public order, public health and for the prevention of commission of crimes or where a delay would present a risk, by the Presidency of Telecommunication, after a request by the Office of the Prime Minister or a ministry concerned with the protection of national security and public order, the prevention of commission of crimes or the protection of public health.

Article 9 provides for a different procedure upon access-blocking/removal of content for the violation of 'personal rights' as a result of personal information which is published on the Internet.

According to the procedure, which is provided under Article 9A, persons who assert that the confidentiality of their private life has been violated by a publication on the Internet may, by applying directly to the Presidency, request that access to that content be blocked.

Consider the rules for the protection of personality. With the advent of mass media, the importance of protecting the honour and dignity within the scope of the right to personality has increased considerably.[2004] Because personal rights are necessarily in conflict with other values, balances must be set carefully. Right to personality is usually conflicting with freedom of the press and Freedom of Expression.

[2004] M Kemal Oğuzman, Ömer Seliçi ve Saibe Oktay Özdemir, *Kişiler Hukuku* (8th edn, Filiz Kitabevi 2005) 135 [Turkish].

Even if there is no reason to comply with the law superior public or personal benefit in Articles 9 and 9/A of Regulation of Publications on the Internet and Combining Crimes Committed By Means of Such Publication Law, it is legally possible for the judge to reject the applicant's request for correction or removal of the content on the grounds that there is a superior and public good in terms of the right to inform the public of the learning of corruption in the concrete case, based on Article 24 of the Civil Code, which prevails in terms of the protection of personality.[2005]

When the current issue is whether the website should be blocked due to unfair competition, the judge shall also listen to the official of the website (or company) that is allegedly violating unfair competition rules and decide whether the website should be closed. In addition, it may be decided to remove the content temporarily instead of blocking the website. Rights protected in private law are personal due to their nature of interest and as a result of this, the court cannot act without the claimant's claim when it is a matter of unfair competition. So, it is possible to say that the judge shall act on demand.[2006]

According to an opinion, access to websites cannot be established based on regulations in other special laws that include an access ban, because the law numbered 5651 is newer and more specific than the mentioned regulations.

In Turkish law, except for the Regulation of Publications on the Internet and Combining Crimes Committed by Means of Such Publication Law, Statue 5651 and the special laws referring to this law, there shouldn't be any access-blocking otherwise, fundamental rights and freedoms will be restricted excessively, disproportionately and arbitrarily.

3.2. Does a context exist in your country under which otherwise legal content may be blocked/filtered or taken down/removed?

It is possible to limit fundamental rights and freedoms in exceptional circumstances. If a war, martial law, or state of emergency is the subject the exercise of fundamental rights and freedoms can be partially or completely stopped or make provisions against the guarantees for them which are stated in the law or even in the Constitution.

An internet site could be banned in an extraordinary period for an unforeseen reason. It is even possible for the administrative authority to completely block internet access during extraordinary periods. While there are very serious discussions in terms of access bans based on the law and judicial decisions in

[2005] Ş Cankat Taşkın, *İnternete Erişim Yasakları* (1st edn, Seçkin 2016) 385 [Turkish].
[2006] Ibid., 399.

ordinary periods, it probably will not be possible to control access-blockings in extraordinary situations and such a situation is incompatible with the rule of law. Turkish Emergency Law[2007] Article 11 paragraph 1-f grants to the state of emergency's regional governor the authority to 'control, record or prohibit speech, text, picture, film, record, audio and videotapes and all kinds of broadcasts made by sound'. The question is 'is it possible for the state emergency's regional governor to access-block the internet in the jurisdiction?'. Even though 'internet' is not mentioned in Turkish Emergency Law Article 11 paragraph 1-f; since 'all kinds of broadcasts made by sound' is mentioned and at the time the law was adopted There was no internet in Turkey, therefore, the governor can exercise its power.

3.3 Which safeguards are in place to ensure a balance between censoring and Freedom of Expression?

The Constitution of the Republic of Turkey ensures the balance between freedom of speech and censorship. On the other hand, in the situation of violation of rules, appeal to the Constitutional Court and European Court of Human Rights also ensures the balance between them.

In Article 13 of the Constitution regulates the restriction of fundamental rights and freedoms. Article 13 of the Constitution refers to the protection and restriction conditions of fundamental rights and freedoms. The criteria of this restriction provide a balance. Accordingly, the restriction can only be done by law and in conformity with the reasons mentioned in the relevant articles of the Constitution without infringing upon essence.

Article 26 of the Constitution regulates the Freedom of Expression and dissemination of thought. This article explicates that the exercise of these freedoms may only be restricted for reasons such as national security, public order, public safety which is individually stated in the Constitution.

According to Article 90 of the Constitution in the case of a conflict between international agreements, the provisions of international agreements should be prioritised related to fundamental rights and freedoms. For this reason, international agreements with Turkey are a part of ensuring this right.

According to Article 13 and 26 of the Constitution, Freedom of Expression can be limited just by law and is subject to Constitution. In this manner, the Constitution makes the restriction of Freedom of Expression more difficult. There are authorities to appeal for violation of this right. These

[2007] Turkish Emergency Law n. 2935 1983 [Olağanüstü Hal Kanunu] [Turkish].

authorities also assure to keep the balance between censorship and Freedom of Expression. In the situation of breach of a right, people have the right to petition the Constitutional Court and European Court of Human Rights.

3.4. Process of judicial review of cases where content has been blocked or taken down from the internet

A decision on access-blocking following the procedure under Article 8 of Regulation of Publications on the Internet and Combining Crimes Committed by Means of Such Publication Law, shall be issued if there are sufficient grounds for suspicion. Searching for sufficient suspicion is more appropriate than seeking simple or strong suspicion, because with simple suspicion, blocking of access may lead to violations of rights, but it will be difficult to start an investigation if strong suspicion is sought.

The decision to block access is made by the judge during the investigation phase and by the court in the prosecution phase. During the investigation phase, it can be decided to block access by the public prosecutor in cases where a delay would present a risk. When the decision on access-blocking is taken by the public prosecutor, this decision shall be submitted to the approval of a judge within 24 hours and the judge shall give his/her decision within a maximum of 24 hours. If the judge does not validate it, the blocking measure is lifted immediately. The lifting of a blocking measure results also from a decision not to prosecute the public prosecutor at the end of the subsequent investigation into the commission of crimes indicated in the first paragraph of Article 8, and from an acquittal decision given by criminal courts at the prosecution stage.

If the decision to block access is deemed qualified to achieve the purpose, it can be made for a limited period. Although the decision regarding the prevention of access as a precautionary measure can be challenged by the provisions of the Criminal Procedure Law, it is not possible to talk about the effective use of the right of objection since the access barrier decision has not been notified to the content providers, and this situation is against Article 36 of the Constitution ; the equality of the weapons principal and principle of fair trial which are specified in Article 6 of the European Convention on Human Rights.

A copy of the decision of access-blocking which is made by the judge, court or public prosecutor shall be sent to the Information and Communication Technologies Authority to apply it.

Under Article 8(4), the Presidency of Telecommunication has competence to issue an ex officio blocking order which is executed by the access provider within a maximum of four hours as from the notification, in two different situations: 1)

the content or hosting provider of the publications with content which constitutes offences as specified in the first paragraph of Article 8 is located outside the country, and 2) the content of publications constitutes offences mentioned in subsections (2) and (5) and (6) of section (a) of the first paragraph of Article 8 (i.e. sexual exploitation of children, obscenity and prostitution), even if the content or hosting provider is located within the country.[2008]

The decision of access-blocking is carried out immediately and within four hours of the notification of the decision at the latest.

In the event that the identity of the publishers, which constitute the subject of the decision to block the access given by the Presidency of Telecommunication, is determined, the Presidency of Telecommunication shall file a criminal complaint with the Chief Public Prosecutor. If there is no need to prosecute as a result of the investigation, the decision of access-blocking will automatically be voided.

If an acquittal decision is made during the prosecution phase, the decision to block access is automatically voided. In this case, a copy of the acquittal decision is sent to the Information and Communication Technologies Authority by stating the internet address subject to the decision to block the access, which is voided by the court.

If the content that constitutes the crimes mentioned in the first paragraph is banned the decision to access-blocking shall be removed by the public prosecutor during the investigation phase and by the court during the prosecution phase.

Those who fail to fulfil the requirement of the access-blocking decision which is given as a precautionary measure, or those responsible for access providers, will be punished with a judicial fine from 500 days to 3 thousand days, unless the act constitutes another crime that requires more severe punishment.

Decisions to block access made under the second, fourth and fourteenth paragraphs of Article 8 are made by the method of blocking access to the content (in the form of URLs) concerning the publication, section, section where the violation occurred. However, in cases where it is technically not possible to block access to content related to the violation, or if the violation cannot be prevented

[2008] European Union: European Commission, European Commission for Democracy Through Law (Venice Commission), Turkey -Law No. 5651- On Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication, 15 June 2016 , CDL-AD(2016)011, para 44.

by blocking access to the relevant content, it may be decided to block access to the entire website.

The amendment of the Internet Law in March 2015 added a new Article 8A providing for an additional procedure for removal of content and/or blocking of access in order to protect the right to life or security of life and property, national security and public order, public health and for the prevention of commission of crimes (Article 8A(1)). According to this provision, access to an Internet site may be blocked by a judge (peace judgeship), or where a delay would present a risk, by The Information and Communication Technologies Authority, subsequent to a request by the Presidency or a ministry concerned with the protection of national security and public order, the prevention of commission of crimes or the protection of public health. The access providers and the content and hosting providers shall be immediately notified by the Presidency of the decision and the blocking or removal measure shall be implemented immediately, within a maximum of four hours as from the notification of the decision. According to second paragraph of Article 8A, any decision for the removal of the content and/or blocking of access issued by the Presidency at the request of the Office of the Prime Minister or the relevant ministries shall be submitted by the Presidency for approval by a magistrate within 24 hours. The judge shall announce his/her decision within 48 hours; otherwise the decision shall automatically lapse. [2009]

Decisions to block the access given under Article 8A are made by the method of blocking access to the content (in the form of URL, etc.) regarding the broadcast, part, a section where the violation occurred. However, in cases where it is technically not possible to block access to content related to the violation or to prevent the violation by blocking access to the relevant content, it may be decided to block access to the entire website.

Article 9 provides for another procedure for access-blocking/removal of content for the violation of 'personal rights' as a result of information published on the Internet. According to paragraph 1, real persons, legal entities and institutions and organisations may, if they assert that their 'personal rights' have been violated, apply for removal of publication of that content by means of a warning to the content provider or, if the content provider cannot be contacted, to the hosting provider, or they may also apply directly to a judge to request denial of access to the content. The judge shall make a decision within a maximum period of 24 hours without holding a hearing. [2010]

[2009] ibid., para 55.
[2010] ibid., para 56.

In line with the demands of those whose personal rights are violated due to the content of the internet broadcast, the judge may decide to prevent access within the scope specified in Article 9.

The judge makes the decisions to block the access to be made within the scope of this article mainly through the method of blocking access to the content (in the form of URL, etc.) in relation to the publication, section, section where the violation of the personal right occurs. However, if the judge thinks that the violation cannot be prevented by specifying the access to the content by specifying the URL address, he can also decide to block access to the entire publication on the website, provided that he justifies the reason.

Access-blocking decisions which are made by the judge under this article are sent directly to ESB (the Access Providers Association.)

Access-blocking decision by the Association is immediately fulfilled by the access provider within four hours at the latest.

In the event that the publication regarding the violation of the personal right subject to the decision of blocking the access given by the judge is published on other internet addresses, the current decision is also applied for these addresses.

Under the procedure provided for in Article 9A, persons who assert that the confidentiality of their private life has been violated by a publication on the Internet may, by applying directly to the Presidency, request that access to that content be blocked. The Presidency shall immediately inform the Union of Access Providers in order to ensure that this request is implemented, and access providers shall carry out the request immediately, within a maximum of four hours. Persons who request blocking of access shall submit their demand for prevention of access to a judge within twenty-four hours of the demand for blocking of access. The judge shall announce his/her decision within a maximum of 48 hours. Further, according to Article 9A, paragraph 8, in circumstances where it is considered that delay may present a risk of violation of the confidentiality of private life, the access-blocking shall be carried out by the Presidency upon the direct instructions of the President. [2011]

3.5. Does the legislation in your country on content filtering and take down conform with the requirements set out in the case law of the European Court of Human Rights?

Turkey is a State party to all major international human rights instruments, including the international Covenant on Civil and Political Rights and the

[2011] ibid., para 57.

European Convention for the Protection of Human Rights and Fundamental Freedoms. The exercise of the Right to Freedom of Expression may be subject to restrictions.

In its Recommendation CM/Rec(2016) on Internet Freedom, the Committee of Ministers of the Council of Europe considered that 'before restrictive measures to Internet access are applied, a court or independent administrative authority determines that disconnection from the Internet is the least restrictive measure for achieving the legitimate aim'. The principle of 'least intrusiveness' is an important element of the proportionality requirement when reviewing the conformity of such restrictions with European and international standards. However, the only measure provided for in Law No. 5651 is the measure of access blocking/removal of content which is the most severe measure possible on the Internet. The Law does not provide for any other measure, less intrusive than blocking/removal, as for instance, requirement of 'explanation' from the interested party (content provider, web-site owner, etc.), 'response', 'correction', 'apology', 'content renewal', 'access renewal' etc. Moreover, the Law does not leave the judge or the Presidency any room for imposing a lower sanction in specific circumstances following a proportionality assessment. Consequently, it is strongly recommended that Law No. 5651 be amended in order to introduce a list of less intrusive measures than access-blocking/removal of content which would allow the judge to make a decent proportionality assessment and apply the least restrictive measures if they are considered as sufficient and adequate to reach the legitimate aim pursued by the restriction. [2012]

The issuing of an access-blocking decision, under both paragraphs (2) and (4) of Article 8, constitutes an interference into the Right to Freedom of Expression that requires justification under any of the grounds and legitimate aims listed in the second paragraph of Article 10 ECHR. The crimes listed in paragraph 1 of Article 8 as grounds for blocking orders appear to be covered by several legitimate aims for restrictions listed in the second paragraph of Article 10 ECHR, as for instance, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, etc. The restrictions under those legitimate grounds, in order to respect the Right to Freedom of Expression, must also be necessary in a democratic society, i.e. they should be suitable to realise the legitimate aims put forward to justify the interference, there should be a pressing social need for the interference and the

[2012] European Union: European Commission, European Commission for Democracy Through Law (Venice Commission), Turkey -Law n. 5651 (Law on Publications on the Internet and Combating Crimes Committed by Means of Such Publication, 15 June 2016 , CDL-AD(2016)011, para 36.

restrictions should be proportional to the legitimate aims pursued and least intrusive into the right.[2013]

Although Article 8 limits the procedure to cases where there is 'sufficient suspicion' of the commission of any of the crimes listed in paragraph 1 and thus satisfies the requirement that the interference must pursue a legitimate aim, it does not mention, explicitly or implicitly, the requirement that the restriction must be 'necessary in a democratic society'. In addition, the provision, according to the English translation, is a 'shall' provision, meaning that a decision to block access will have to be issued in case the internet publication contains any of the content listed there. However, the resulting interference with the Freedom of Expression is only justified if it is necessary for the protection of any of the interests listed in the second paragraph of Article 10 ECHR and if it meets the proportionality requirement. In order to be 'necessary in a democratic society', the 'interference' with the Freedom of Expression should correspond to a 'pressing social need' and be proportionate to the legitimate aim pursued while the reasons given by the national authorities to justify it should be relevant and sufficient. Especially in view of the far-reaching restrictions as a wholesale blocking of a site regardless of its present and future content, but also in case of blocking orders concerning a precise content (URL address), the test of proportionality is of vital importance when reviewing the conformity of such restrictions with European and international standards. [2014]

The provision does not provide for any notification procedure of the interested party about the procedure under Article 8(2). The authorities explained that the name of the court or authority that implement the order of access blocking, is displayed on the relevant page of the website whose access is blocked due to violent content and the concerned party is consequently informed about the access blocking measure. However, the Commission stresses that this is not sufficient and a proper notification procedure should be put in place in order to give the content providers the opportunity to have knowledge of the blocking measure and of the reasons put forth by the authorities to justify the measure. The principle of 'equality of arms' implies that each party must be afforded a reasonable opportunity to present his/her case – including his/her evidence- under conditions that do not place him/her at a substantial disadvantage vis-à-vis the other party. Furthermore, it is clear under the case law of the ECtHR that it is inadmissible for one party to make submissions to a court without the knowledge of the other and on which the latter has no opportunity to comment. It is strongly recommended that the provision be amended to impose on the

[2013] ibid., para 45.
[2014] ibid., para 48.

authorities the obligation to notify the interested party about the access-blocking measure and its reasons. This is all the more important in view of the heavy fines imposed on the access/hosting providers for failure to implement the blocking decisions taken as precautionary or administrative measure under para 10 and 11 of Article 8.[2015]

The removal of content from and the blocking of access to the Internet constitute restrictions of the Right to Freedom of Expression that require a justification on any of the grounds and on the conditions listed in the second paragraph of Article 10 ECHR. According to this provision, any restriction must be prescribed by law and necessary in a democratic society in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[2016] Paragraph 1 of Article 8A meets the first two sets of requirements in so far as it constitutes a legal basis for the removal and blocking measures, and lists more or less the same limitation grounds (i.e. legitimate aims for restrictions) as those enumerated in the relevant international legal provisions. Nevertheless, the requirement that the restriction must be 'necessary in a democratic society', i.e. the 'interference' into the Freedom of Expression should correspond to a 'pressing social need', and be proportionate to the legitimate aim pursued, and that the reasons given by the national authorities to justify it should be relevant and sufficient, is not mentioned in paragraph 1 of Article 8A. The Venice Commission takes note of and agrees with the concern of the authorities that the Internet can be used in particular by criminal organisations to pursue and facilitate their criminal activities. However, the fact that the interference pursues one or several of the legitimate aims for restriction stipulated in paragraph 1 of Article 8A is not sufficient (the justification is not automatic). In addition to those legitimate aims, the interference should also fulfil the requirements of 'democratic necessity'. In this respect, when applying blocking/removal measures, the competent authority (judgeship or the Presidency) should take into account the ECHR case law concerning in particular the freedom of political speech , which requires a high level of protection of the right to Freedom of Expression and enables everyone to participate in the free political debate which is at the very core of the concept of a democratic society.[2017] The blocking or removal measures following procedures under Articles 9 and 9A raise the issue

[2015] ibid., para 51.
[2016] ibid., para 64.
[2017] ibid., para 66.

of fair balance which should be struck between, on the one hand, the protection of Freedom of Expression. The ECtHR has laid down the relevant principles which must guide its assessment in this area. It has thus identified a number of criteria in the context of balancing the competing rights: contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication etc. Consequently, the fact that the interference into the Right to Freedom of Expression (blocking orders/removal of content) pursues the legitimate aim of protection of rights of others is not sufficient while, in addition to this legitimate aim, the interference should also fulfil the requirements of 'democratic necessity', i.e. a fair balance should be struck between Freedom of Expression and the protection of private life/personal rights. Nevertheless, the requirement of 'democratic necessity' and its components 'fair balance' and 'proportionality' are not mentioned in Articles 9 and 9A.[2018] The ECtHR has held that Article 10 ECHR does not prohibit prior restraints on publication as such. It has stressed, however, at the same time, that the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court. The Court emphasised that this is especially so as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest, but that this danger also applies to other publications that deal with a topical issue. The foregoing means that the conditions for the justifiability of restrictions of the Freedom of Expression have to be interpreted and applied even more restrictively in cases where the restrictions have an undifferentiated (complete denial of access to the internet site) and a preventive character in blocking access to future information and communication. In Article 8A and 9, the decision to block the whole website should be 'proportionate' and supported with exceptionally strong arguments that the blocking measure does not cross the boundaries of what is strictly necessary in the specific concrete circumstances of each case.[2019]

3.6. Relevant Case Law: Wikimedia Foundation Inc. and Others

BTK (Turkish Information and Communication Technologies Authority) has instructed Wikipedia to remove two different contents from its website. These contents were on the topics of the Stated Sponsored Terrorism and the Foreign Involvement in The Syrian Civil War. BTK justified its order for the removal of contents with the arguments that the contents pose a threat to Turkey's internal

[2018] ibid., para 67.
[2019] ibid., para 68.

and external national security and have a potential for disturbing the public order. BTK blocked access to the content on 29 April 2017, under the exceptional authority provided in the current law. Access to Wikipedia has been completely blocked due to the fact that it is not technically possible to remove the two specified URL addresses. Wikimedia Foundation Inc. and Others applied to the Constitutional Court by claiming that their fundamental rights were infringed with BTK's decision. As a result, the Constitutional Court decided for the violation on 26 December 2019. The Constitutional Court ruled that the Freedom of Expression guaranteed by Article 26 of the Constitution is violated as a result of BTK's decision. In this period, the access of Wikipedia was blocked more than two and a half years. The Constitutional Court stated that BTK's blocking of access was not within the scope of the exception. Deterioration of state dignity is not a concrete justification under current law.

3.7. Relevant Case Law: YouTube LLC Corporation Service Company

BTK has determined that there is an insult to Mustafa Kemal Atatürk at 15 URL addresses available at YouTube platform and BTK sent a warning message to YouTube for removing these contents. Access to YouTube website was blocked because the contents have not been removed. Thereupon, the criminal court of first instance decided to remove the decision for blocking the access to YouTube excluding to the address of 15 URL which were considered as having libellous contents. BTK has not followed this decision. BTK's action was challenged before the administrative court, and the administrative court has decided to stay the execution of the decision for blocking of access. BTK did not implement the court order. The applicants then applied to the Constitutional Court individually. Turkish Constitutional Court's decision rendered on 29 May 2014 concluded that the Freedom of Expression of the applicants guaranteed under Article 26 of the Constitution was violated.

In this case, domestic remedies were not exhausted. However, it was concluded that there is no effective way of application because the administration (BTK) has not implemented the court order.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

4.1 Legal Basis of Blocking/Taking Down Internet Content

The taking down or blocking of contents published via internet is regulated with the law No. 5651 on Regulations of Internet Contents and Fighting Against

Crimes Committed via Internet Contents, which was legislated in 2007. As the law requires, the content may be taken down or blocked in case of one or more of the followings occur:

- Infringement of personal rights
- Committing actions considered as crimes
- Infringement of privacy
- Infringement of law no.5846 on Intellectual Property Rights
- Usage of the right to be forgotten
- Infringement of public peace

Law Regulations on Internet Contents and Fighting Against Crimes Committed via Internet Contents numbered 5651, requires a judicial process and does not mention a self-regulation mechanism.

4.2. Legal Basis of Self-Regulation

Although Freedom of Expression is protected by the Constitution Article 26, no safeguard in place for ensuring the protection of Freedom of Expression online is applied under Turkish regulations in case of self-regulated censorship. The private sector is considered totally free to avoid contents considered as inappropriate, even if the content is suitable according to the law.

However, there are laws that mention but not limit self-regulation. Law No.6112 on the Establishment of Radio and Television Enterprises and Their Media Services mentions the concept of self-regulation. Article 22 in chapter 6, titled 'Private Media Service Providers' is as follows: Media service providers shall assign a viewer representative who has at least ten years of professional experience in order to establish co-regulation and self-regulation mechanisms to submit the evaluations on the complaints obtained from viewers and listeners to the editorial board of the company and to follow up the conclusions. The assigned viewer representative shall be announced to the public by appropriate means and notified to the Supreme Council.[2020]

In addition, in the first chapter of the same law, Article 37 which is on the duties and powers of the Radio and Television Supreme Council, it is regulated as the following: to keep abreast of developments concerning the media services; Article 014 on general and specific broadcasts to determine co-regulatory and self-regulatory mechanisms and general strategies for the sector; to conduct

[2020] Medya Kitaplığı, '*Media Self Regulation in Turkey; Challenges, Opportunities, Suggestions*', <platform24.org/en/Content/Uploads/Editor/Media%20Self-Regulation%20in%20Turkey.pdf> accessed 25 May 2020.

studies and to provide incentives in order to ensure improvement of media services in the country; to coordinate educational and certification programs for employees of media service providers, and to issue certificates.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

The Right to be Forgotten is called for the recognition by European policymakers in other words it is a legal concept much discussed and put in the practice in the European Union. This right provides an individual to request deletion of old personal data that one wants no longer to be known from the digital memory.

In 2014 'the Right to be Forgotten' also known as 'the Right to Oblivion' became a current issue because of the Court of Justice of the European Unions' decision about *Google v. Spain* case.

General Data Protection Regulation is current legislation that applies in EU member Countries, the right to be forgotten is specifically stated in GDPR.

In Turkish Law, the right to be forgotten is not a specifically legislated right. Although there are not any legal restrictions about the subject. If a Turkish citizen applies to these web search engines to remove, delete or restrict a personal data the legal tools in Turkish Law are 'Turkish Personal Data Protection Law no. 6698[2021]' and 'Law on Regulation of Broadcasts Published on the Internet and Intervention of Crimes Committed Through These Broadcasts no.5651'.[2022] Application of the Right to be Forgotten in Turkey is not restricted with these two statutes; there are also other secondary regulations that can be used to solve a dispute. In addition to legislations above mentioned, there are other legislations that in Turkish law can be apply to the subject. These legislations are Law of Intellectual and Artistic Works (Law no. 5846 of December 5 1951)[2023], Turkish Criminal Code (Law no.5237 September 26 2004)[2024], Turkish Commercial Code (Law no.6102 January 13 2011)[2025], Turkish

[2021] Law n. 6698 (Turkish Personal Data Protection Law) 2016 [Kişisel Verilerin Korunması Kanunu].
[2022] Law n. 5651 (Law on Regulation of Broadcasts Published on the Internet and Intervention of Crimes Committed Through These Broadcasts) 2007 [İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun].
[2023] Law n.5846 (Law of Intellectual and Artistic Works) 1951 [Fikir ve Sanat Eserleri Kanunu].
[2024] Law n. 5237 (Turkish Criminal Code) 2004 [Türk Ceza Kanunu].
[2025] Law n. 6102 (Turkish Commercial Code) 2011 [Türk Ticaret Kanunu].

Law of Obligations (Law no. 6098 1 January 2011)[2026], Turkish Civil Law (Law no.4721 22 November 2001)[2027].

In Turkish Law, closest legislation to the Right to be Forgotten takes place in Turkish Personal Data Protection Law Article 7 titled as 'Deletion, Destruction, and Anonymization of Personal Data' which provides individuals to appeal to a court for these actions which could be provided by the decision of prospective judgment of the court. With that article Turkish legislators creates content of the Right to be Forgotten under the roof of different legislations that contains the protection of personal data. The legislations that creates the essential components of the Right to be Forgotten can be seen in various articles that mentioned before. The Right to be Forgotten can be observed within these various Laws in Turkish Law, on the other hand European Union has different aspect about the Right to be Forgotten. European Union creates specific legislations either protection of personal data or the Right to be Forgotten. The basic regulation of the protection of personal data in the European Union is contained by Directive 95/46/CE of the European Parliament and the Council dated 24 October 1995 regarding the protection of natural persons in what concerns the processing of the personal data and the free circulation of such data and the Right to be Forgotten appears in Recitals 65 and 66 and in Article 17 of the GDPR. It states, 'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay' if one of several conditions applies. You must also take reasonable steps to verify the person requesting erasure is actually the data subject[2028]. The concept as a protection of personal data in scope of using the Right to be Forgotten can be assured via those regulations in EU member countries. While these regulations being accepted by EU member countries, Turkish legislators begin to add new articles about the protection of personal data by minor Constitutional changes. On May 2010, Turkish legislator introduced an additional paragraph related to the protection of personal rights. Turkish Constitution Article 20/3 states that 'everyone has the right to request the protection of his/her personal data'. Turkish legislators' intention to adding essential components of the Right to be Forgotten can be seen in continued sentences in this Article. Such as 'This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged

[2026] Law n. 6098 (Turkish Law of Obligations) 2011 [Türk Borçlar Kanunu].

[2027] Law n. 4721 (Turkish Civil Law) 2001 [Türk Medeni Kanunu].

[2028] '*Everything You Need to Know About 'the Right to be Forgotten'* https://gdpr.eu/right-to-be-forgotten/ accessed 25 May 2020.

objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law.'. Turkish legislators' intention to create a legal basis to protection of personal data in scope of the Right to be Forgotten has several similarities with Article 17 of the GDPR.

Also, the right to be forgotten is not processed in 'Turkish Personal Data Protection Law Draft'. In this context we can understand that Turkish legislators are not intended to create a specific legislation about the right to be forgotten. Disputes related to violation of the Right to be Forgotten can be concluded in Turkish Courts with the notion of protection of personal data[2029], privacy and protection of private life[2030] and suspension of the exercise of fundamental rights and freedoms[2031]. These notions are regulated in the Turkish Constitution and laws above mentioned.

Being a non-EU member country, Turkey's position of applying the right to be forgotten is not clear. On the other hand, like any other non-EU member country, Turkey's position will become clearly understandable through time. In this context, Turkey's position of applying this right in court decisions recently increased. According to Turkish Constitution Article 141/3, all decisions of all courts should be written with a justification.

These decisions can be seen as a beginning of using the right to be forgotten in Turkey, as a legal concept.

5.1. Some Legal Issues About The Right to be Forgotten in Turkish Law

Judicial decisions that are published without deleting personal information, online news that violate personal rights and despite the overriding public interest creating obstacles to prevent reaching online information are legal issues that Turkish Courts stated decisions about the right to be forgotten (or related to the subject).

The first decision that stated the right to be forgotten as a legally known right is a Supreme Court of Appeals' Decision (2014/4-56, 2015/1679, 17.06.2015)[2032]. In this case, plaintiff's counsel stated that her/his client is making a complaint about being a victim of sexual assault after publishing the court order the plaintiff sees his/her client's name and other names that related the case. This court order was used inside as a legal material in a Criminal Law book. As a result

[2029] Law n. 6698 (Turkish Personal Data Protection Law) 2016 [Kişisel Verilerin Korunması Kanunu].
[2030] Constitution of the Turkish Republic 1982 [Türkiye Cumhuriyeti Anayasası], Article 20.
[2031] ibid, Article 15.
[2032] Case n. 2014/4-56, Supreme Court Assembly of Civil Chambers [2015] [Turkish].

of this plaintiff's counsel requested immaterial compensation that caused the violation of hers/his client's personal rights. Defendant's counsel claimed that these books have scientific value and it is going to be used only by a small number of people that have interests about the related subject. The court decided on the grounds that plaintiff's name's is being directly written instead of using encrypting or codes is harms plaintiff's personal rights, especially when Turkish society's aspect about sexual assault considered there is not any scientific benefits could be provided from this publishing behaviour.

In order to be able to obtain the specific effects of the 'Right to be Forgotten', at least one of the following conditions must be fulfilled: the data is no longer required for the scope was processed or collected for. The scope of collection must be, at its turn, specified, explicit and legitimate. Any subsequent processing shall have to be compliant with the scope; the concerned person retracts his or hers consent for one or more specific scopes on which the processing is based, or when the storage period for which the consent was given has expired and there is no legal ground for processing the data; the concerned person makes an opposition to the processing of the personal data for reasons related to his particular situation, when this processing is necessary for protecting the vital interests of the concerned person, executing a task of public interest or for the execution of the official authority wherewith the operator was invested or fulfilling the legitimate interest of the operator, except for the cases when this interest is less important than the interests or rights and fundamental liberties of the concerned person that require the protection of the personal data, particularly when the concerned person is a child; processing the data is not compliant with the provisions of the regulation for any other reasons whatsoever.

There are some exceptions relating to the Civil Law. These exceptions can be applicable in Turkish Law if the court sees it necessary. There are provisioned cases when the operator is exempted from the obligation to delete the personal data on demand, namely when these data are necessary: for exercising the right to free expression. In order for this exception to be applicable, the processing of the data shall be performed only for journalistic, artistic, literary scopes. On grounds of public interest regarding the public health, when the personal data are necessary for preventive medicine, labour medicine, diagnosis, treatment, health services management, with the observance of the professional secrecy, other reasons of public interest, such as social protection, especially for granting the quality and competitiveness of the proceedings for the settlement of the claims for benefits and services related to the health insurance system; on historical, statistic or scientific grounds, only if the pursued scope cannot be

achieved, by processing the data which does not allow or not allow anymore the identification of the concerned person and the data allowing the assignment of the information to a concerned identified or identifiable person is being kept separately from the rest of the information as long as the scope can be achieved in this manner; for the observance of a legal obligation to retain the personal data imposed by the European Union legislation or by the national law of the operator; in those cases where instead of deletion, the operator restricts the processing of the personal data, respectively when the accuracy is contested by the concerned person, while they are verified, the operator does not need anymore the personal data for achieving his goal, but he must preserve them as evidence, the processing of the data is illegal and the concerned person opposes to the deletion, requesting the restriction of the use instead or the concerned person requests the transmission of the data to another automatic processing system, in case the concerned person provided the personal data and their processing is performed based on his or hers consent or on a contract.

In addition to Civil Law's aspect about the exceptions about this right there are some remarks that stated especially the Turkish legislators' perspective.

According to this the first prohibition in Turkish Law is indicated in Turkish Construction, with the Article 14 Turkish legislator aims to prevent abuse of using fundamental rights and freedoms. That can be seen as a more protected aspect of law than the Right to Forgotten' direct applicability as a specific legislation. Article 14's title is 'Prohibition of abuse of fundamental rights and freedoms' to use interpretation to understand Turkish Legislator's intention: the need to create a legislation about the Right to be Forgotten shouldn't be overlooked.

In conclusion, we can observe that even though there is not any specific legislation about the Right to be Forgotten in Turkish Legal System, this right is acknowledged by Supreme Court Practice, this provides individuals to use this right with applying litigation in the Turkish Courts.

6. How does your country regulate the liability of internet intermediaries?

One of the most fundamental concepts of Internet regulation in Turkey is liability of internet intermediaries. Different intermediaries are subject to different liability regimes within the scope of Act 5651, known as the Internet Act carried out by Information and Communication Technologies Authority.

Internet intermediaries include:

— Internet access and service providers (ISPs)

— Data processing and web hosting providers, including domain name registrars

— Internet search engines and portals

— E-commerce intermediaries, where these platforms do not take title to the goods being sold

— Internet payment systems

— Participative networking platforms, which include Internet publishing and broadcasting platforms that do not themselves create or own the content being published or broadcast

Within the scope of this study, most relevant intermediaries are participative networking platforms, i.e. social media platforms and Internet Service Providers.

6.1 Obligation to implement the measures for blocking and taking down content

Internet intermediaries are exposed to administrative fines unless they implement the measures for blocking and taking down content. There is Article 4 for content providers, Article 5 for host providers, Article 6 for access providers, Article 7 for mass use providers and Article 8 for blocking measures. Main obligation of access, content and hosting providers is that the provider must furnish the Presidency of Telecommunications any information as it may demand without the need of a court decision. Also, the blocking actions of the Presidency of Telecommunications are lack of judicial evaluation.[2033]

6.1.1. Service Providers

Internet service providers are the backbone of the Internet based communications, it is the ISPs that operate web. Therefore, ISPs are the direct addressee of any blocking or filtering and such government actions and regulations. In this sense ISPs have a key role in enabling expression, as they are the ones that facilitate or restrict Freedom of Expression.[2034] Liability of service providers is provided in the Article 6 of Act 5651, the article mentions the obligations of service providers. ISPs were highly affected by the modifications

[2033] Gürkaynak, Gönenç, and Yılmaz, İlay. *New Access Ban Regime Proposed for Law 5651'* (Globe Business Media Group, 24 March 2015) <www.gurkaynak.av.tr/docs/New-access-ban-regime-proposed-for-Law-5651.pdf.> accessed 10 May 2020.

[2034] MacKinnon, R., Hickok, E., Bar, A. and Hae-in Lim, *Fostering Freedom Online: the Role Of Internet Intermediaries* (Paris: UNESCO 2014).

to the Internet Act, which made the procedure of blocking much easier than before. According to the omnibus bill that modified the Act, the prime minister and any ministries may soon be given the power to request TIB to block websites within four hours. Upon governmental request, TIB will be able to take urgent measures to block access to websites or remove online content for 'protecting the right to life, protecting people's life and property, national security, public order, preventing crime, or protecting general health'. Websites must be blocked by service providers within four hours from TIB's communication of the Government's request and will remain blocked until the content is removed. [2035]

6.1.2. Content Providers

Content providers are regulated through Article 4, the liability regime suggests that content providers are responsible for the content they create, and publish through their own

websites, yet they are not liable for third party content that they provide linkage to. This situation indeed, paves the way to overall blocking of the pages because Turkish Internet Law clearly indicates that blocking measures are applied to specific URLs, only when it is technically impossible to block a single URL, the Information and Communication Technologies Authority allows for the blocking of the whole website. (Article 8/2) However, Article 8/4 suggests that URL filtering technology for foreign-based websites is not available in Turkey. As most of the social media platforms are based abroad, rather than blocking URLs, the government blocks access to the website. Access to many websites from Twitter to YouTube and the most recent one Wikipedia, has been banned in Turkey more than once. Another option is to submit a legal request to remove content from the provider. This is another problematic point for Turkey, especially on Twitter. The 2019 Transparency Report of Twitter shows that Turkey is the second following Russia in global censorship. Twitter reports that: 'We filed 75 legal objections with Turkish courts in response to 388 court orders, on the grounds that these orders did not comply with the principles of freedom of speech, freedom of press, and/or did not specify the content at issue. Two of these legal objections were partially accepted on the basis that it would be

[2035] Giancarlo Frosio, 'Intermediary Liability Updates from Turkey: Forcing Online Intermediaries to Create a Website Blocking-Friendly Infrastructure.' (The Center for Internet and Society, 28 January 2015) <http://cyberlaw.stanford.edu/blog/2015/01/intermediary-liability-updates-turkey-forcing-online-intermediaries-create-website> accessed 10 May 2020.

disproportionate to require Twitter to withhold entire accounts instead of specific Tweets.'.[2036]

6.1.3. Hosting Providers

Article 5 of the Act 5651 presented a notice-based liability framework. The article expresses that there is no general obligation to monitor the information which the hosting companies store, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity. [2037] Article 5(2) obliges the hosting companies to take down illegal or infringing content once served with a notice through the Presidency of Telecommunications, or subject to a court order with regards to Article 8 of Law No. 5651.

6.1.4. Access Providers

Article 6/2 states that access providers are not obliged to monitor the information that goes through their networks, and they do not have a general obligation to actively seek facts or circumstances indicating illegal activity concerning the transmitted data. [2038]

6.1.5. Mass Use Providers

Mass use providers are regulated in Article 7, according to the article the providers can only operate with an official activity certificate obtained from a local authority. It is required for mass use providers to deploy and use filtering tools recognised by the Presidency of Telecommunication for blocking access to illegal content on the Internet. Administrative fines Those who operate without an official permission would be subject to administrative fines.[2039]

6.2. Safeguards in place for ensuring the protection of Freedom of Expression online

Despite the efforts of Turkish government for increasing Internet censorship, The Constitutional Court is the very safeguard ensuring the protection of Freedom of Expression online. The Constitutional Court Annulled Article 8/16 on ground that violation of Article 2(Rule of Law), 13 (Restriction of

---

2036 Twitter,'*Removal Requests'*<transparency.twitter.com/en/removal-requests.html> accessed 10 February 2020.

2037 Akdeniz, Yaman. *'Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship.'* OSCE , Organization for Security and Co-Operation in Europe The Representative on Freedom of the Media, <www.osce.org/fom/41091?download=true.> accessed 10 May 2020.

2038 *Ahmet Yıldırım v. Turkey* no 3111/10 ECHR [2012].

2039 ERGUN, Fevzi Doruk. *'National Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy.'* Edam, 3 Apr. 2018, <www.edam.org.tr/en/national-security-vs-online-rights-and-freedoms-in-turkey-moving-beyond-the-dichotomy/> accessed 10 May 2020.

fundamental rights) and 20 (Right to Privacy) of the Constitution.[2040] Highlighted point in the judgment of the court is that the Rule of Law necessitates the principle of 'clarity', meaning that legal arrangements must be clear, unambiguous, comprehensible and applicable and they must also include safeguards against arbitrary behaviour by public authorities. The Constitutional Court held that any restriction of confidentiality and protection of private life must meet the test of proportionality laid down in Article 13 of the Turkish Constitution. The Court also ruled that the provisions gave permission to all kinds of personal data and documents of individuals to be transferred to the Presidency of Telecommunication unconditionally.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1. Analysing The Current Legal Situation in Turkey, Expectable Regulations and De Lege Feranda

Internet Technologies have been developing and renewing so fast and that is actually why it is not predictable to guess what will happen through this subject. However, it is still possible and also needed to regulate national or international law, set up new codes and rules in this subject and adopt them into the legislations.

Criminal issues under Information Technology are mostly solved by following negotiation methods and there are international corporations among the countries on this. Thus, the real and biggest problem in the Internet Technologies area is especially pertinent to the contents since countries have differences about the applicable law for the unlawful acts/torts through the Internet, the points of view, cultural structure, and many more. This part of the research study will focus on the expectations and predictions on what can be legal innovations and regulations in Turkey and which points would be remarkable for the law de lege feranda.

Despite the fact that child porn issues may be considered the only common point in the policies of the countries, each country might have various thoughts

[2040] Official Gazette of Turkish Republic, 1 Jan. 2015, <https://www.resmigazete.gov.tr/eskiler/2015/01/20150101-16.pdf?utm_source=ELIG%20Attorneys%20at%20Law&utm_content=ILO%20newsletter%2030985&utm_medium=pdf&utm_campaign=ILO%20Newsletters> accessed 10 May 2020 [Turkish].

on personal rights and freedoms, and this is the base of blocking, censorship or other types of the sanctions in question in this study. In order to consider the future of Turkish legislation and precedents, it is also mainly needed to have a short look at the past and current rules, precedents, and life-conditions in the country.

First legal rules which restrict the rights and freedom by the internet were intended to amend Criminal Law and Criminal Procedure Law. The commission within the Ministry of Justice, however, was not efficient in working on the legislation and setting up these new rules to prevent child abuse and porn. In addition, Non-governmental organisations aiming to improve Information Technology could not have a chance to take an active role in the legislation process in spite of being the main requirement of democracy.

Blocking domain name was the first manner in the internet area to overcome the arising infringements related to Information Technology. In other words, the authority blocked the whole service providers rather than blocking content partially. This is one of the dangerous restrictions in human rights since more than one person is involved in the websites or there is more than one user of those service providers. Therefore, this manner is beyond the aim and unlawful. The next step as a sanction in this purpose was banning IP numbers. Nevertheless, banning IP numbers means preventing the domain names under the same IP number from being active, and that is obstruction of many users or bloggers just because of one illegal content.

The most well-known examples of blocking IP number or domain name instead of a content blocking were blocking YouTube and Twitter only just because of one video and post. This caused many people in Turkey to be affected negatively in terms of freedom of speech because of someone's liability of internet intermediaries. On the other hand, blocking or taking down an international domain name or IP number must be also evaluated under international law even if it occurs in a country. Limiting access on the Internet somehow most of the time results in international consequences, like in YouTube, Twitter and Wikipedia, which are more recent examples. Therefore, the first conclusion, regarding the previous solutions in Turkey, to find the right sanction for the liability of internet intermediaries is the fact that it should not be ignored by probable international and diplomatic results besides breaching fundamental human rights.

After a short time from the Twitter example in 2014, the Constitutional Court meaning the Supreme Court of Turkey made a decision that such blocking cannot be legal and lawful. According to the court decision; blocking a social

media network is considered 'unlimited restrictions' and it is an obstacle for providing freedom of speech in a democratic society.

Furthermore, these kinds of restrictions through the Internet shall be allowed only in the case that it is needed to be interfered with by the court in an effort to prevent the violations of another fundamental right or in case of emergency. To be able to estimate such cases, the criteria are being 'prima facie'. Supreme Court of Turkey has several precedents like this, so this situation indicates that there would be many more decisions on the same path in the future.

Another point is that the academicians, lecturers, and scientists in Turkey complain about content blocking and internet censorship since their right to access information will be directly influenced. Actually, it can be regarded as the same for all people when we take our century and recent or also future IT developments into our consideration. On the other hand, accessing the Internet is today perceived as another fundamental right of human-being.

For the purpose of analysing how online blocking and liabilities of internet intermediaries will develop in Turkey in upcoming years, another requirement to consider is the relation and balance between the branches of law, such as intellectual property rights and freedom of speech in a case of Internet censorship. For instance, in some cases concerning the new European Copyright Directive, it is conflicted with some assertion of copyright, but actually, massive censorship to be stopped. Therefore, in such a case, it is assumed a hidden danger in the new European Copyright Directive. So, it should be noted that it is always needed to regard predictable or probable issues causing a conflict between different legal domains when working on new international regulations in the near future. This means that besides the small connection and relatively collateral aim between restriction of someone's freedom of speech and protection of copyright in some cases, also some significant and illegal or extracanonical influences on other people may arise.

Apart from setting up a balance between restriction of freedom of speech and protection of copyright, another required balance and proportionality with such blockings is associated with personal data protection leading to access blocking to some websites. General Data Protection Regulation (GDPR) is the main source of this issue. However, Turkey is currently not an EU country, in principle, the EU's General Data Protection Regulation (GDPR) is not directly applicable in Turkey. However, since the territorial scope of the GDPR applies where the personal data processing activities are related to the offering of goods or services to data subjects that are in the Union by a controller or processor not established in the Union, data controllers located in Turkey might be required to

comply with the GDPR. In the purpose of this, Law on the Protection of Personal Data No. 6698 (the DP Law), which constitutes the main legislative instrument that specifies the principles and procedures concerning the processing and protection of personal data, has been published in the Official Gazette on 7 April 2016 and is in effect as of this date.

The protection of personal data is recognised as another fundamental right under Article 20(3) of the Constitution of the Republic of Turkey as of its amendment in 2010. Since the aforementioned Article requires that the principles and procedures regarding the protection of personal data shall be laid down in law; the constitutional guarantee for the protection of personal data is intended to manage the processing of personal data on a regulatory level.

The data protection authority established by the DP Law, the Personal Data Protection Board (the Board), is currently active and has been regularly publishing secondary legislation of the DP Law as well as principle decisions and guidance documents concerning the application of the DP Law. The Board is continuing its work to create public awareness on the issue. Data protection has been an active legal area since the enactment of the DP Law.

The 'right to be forgotten' is not explicitly recognised as a right under the Turkish Constitution. However, the recent case law of both the Penal Department [2041] and the Supreme Court[2042] have ruled that the individuals have a 'Right to be Forgotten' under 'the right to protection of honour and reputation' and 'the right to protection of personal data'. In both decisions, the courts made a reference to the ground-breaking Google Spain judgment of the ECHR. Consequently, it can be said that a right to be forgotten is emerging by way of case law in Turkey. Moreover, the DP Law recognises that individuals have the right to request deletion or destruction of their personal data under Article 11. Thus, data subjects may request their data to be deleted if the reasons for processing no longer exist.[2043]

In the lights of all mentioned expressions above, it is expected that specialised courts on IT Law will be likely constructed to build up IT law issues or cyber-security with the court decisions.[2044] However, for the specialisation Turkish authorities must come together with non-governmental organisations and

---

[2041] Decision n. 2017/5325 Penal Department no 12 of the Supreme Court[2017] [Turkish].

[2042] App. n. 2013/5653 Supreme Court [2013] Official Gazette No. 29811 and dated 24 August 2016 [Turkish].

[2043] The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 (The Law Reviews, October 2019).

[2044] Güven Köse, '*Internet'te Sansür Üzerine Bir Değerlendirme'*, Hacettepe Üniversitesi, <https://www.academia.edu/1614699/Internette_Sans%C3%BCr_%C3%9Czerine_Bir_De%C4%9Ferlendirme?auto=download > accessed 10 May 2020 [Turkish].

professionals on all the topics in question here. It can be predicted that this kind of a new commission is inevitable for the legislation of Turkey in next five years (although it could not be fairly possible with Law No 5651). It is more likely to constitute specialised courts by following this step. Moreover, it seems that if the courts order object-based blocking rather than blocking the whole access to the internet, IP number or domain names, a few big parts of the problems about internet censorship or online blocking will be handled.

It should not be forgotten that any step aiming to achieve fair trial and provide justice will have to be statutory to previous court precedents, the Constitution and international law elements. Thus, that means everything aiming any restriction of fundamental rights will be still having to be in a compatibility with the principle of proportionality[2045] when there is a conflict between the rights. In addition, courts, in this respect, will seek 'prima facia' principle incoming years as well.

Lastly, it is also expected for the Republic of Turkey to strength its legal instruments in the similar line of European Union regulations depending on diplomatic relations.

8. Has your country reached an adequate balance between allowing Freedom of Expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

8.1. Censorship

As of today, there is no agreed-upon definition on censor or censorship in Turkish legislation and legal academia. However, the expression 'censor' has been mentioned in the Constitution. In Article 28 paragraph I of the Constitution states that 'Press is free; it cannot be censored.'

However, the Turkish Constitutional Court has been defining what actions are considered as censorship with its decisions. In an application, the Turkish Constitutional Court evaluated the claims and assessments of companies as commercial expressions. In cases where commercial expressions concern the

[2045] Restriction of fundamental rights and freedoms, Article 13 : (As amended on October 3, 2001; Law n. 4709) Fundamental rights and freedoms may be restricted only by law and in conformity with the reasons mentioned in the relevant articles of the Constitution without infringing upon their essence. These restrictions shall not be contrary to the letter and spirit of the Constitution and the requirements of the democratic order of the society and the secular republic and the principle of proportionality.

society closely with the public interest, the elimination of the opportunity to spread the expression without any justification is evaluated as 'censorship'.[2046]

The expression 'censorship' has been usually understood within the context of the press, whether it is published on paper or on the internet. In recent decisions, the Turkish Constitutional Court has developed an approach on balance between Freedom of Expression and censorship.

The harmony between the production, distribution and presentation of thought and Freedom of Expression goes hand in hand. Therefore, in order to talk about Freedom of Expression, it is necessary not to interfere with the disclosure of thought in different mediums as well as with other persons' access to the expression. On the contrary, the prevention of thought, information and public material that may be considered as objectionable and dangerous by individuals, groups and government officials will result in censorship that results in banning creativity and freedom of thought.[2047]

According to the opinion of the Turkish Constitutional Court, to categorically restrict access to certain information published on the internet or to categorically block the information and documents that are intended to be published have the characteristics of censorship. Therefore, it will be evaluated as censored to prevent categorical access to news or thoughts published on the internet because they are related to a particular event.[2048]

Censorship makes it impossible to create a ground for public debate on important social issues. As a result, the censorship stemming from the preventing measures weakens the belief in the state of law, creating the impression that the incident was covered up. In this respect, the margin of appreciation of the state in the interventions on Freedom of Expression on the issues similar to the subject of the application is quite limited and cannot be accepted in accordance with the requirements of the democratic social order unless it is due to a compulsory social need and proportionate.[2049]

8.2. Right to Information

With the amendment made in the Turkish Constitution in 2010, the right to information is clearly recognised in the Article 74, even though it is not regulated

---

2046 *Medya Gündem Dijital Yayıncılık Ticaret A.Ş.* [2013] Constitutional Court of the Republic of Turkey 2623 [2015] [Turkish].

2047 *Birgün İletişim ve Yayıncılık Ticaret A.Ş.* [2015] Constitutional Court of the Republic of Turkey 18936 [2019] 81 [Turkish].

2048 *App. n. 2015/18581*, Constitutional Court of the Republic of Turkey [2019] 51; *Birgün İletişim ve Yayıncılık Ticaret A.Ş.* [2015] Constitutional Court of the Republic of Turkey 18936 [2019] 82 [Turkish].

2049 *App. n. 2015/18581*, Constitutional Court of the Republic of Turkey [2019] 53; *Birgün İletişim ve Yayıncılık Ticaret A.Ş.* [2015] Constitutional Court of the Republic of Turkey 18936 [2019] 82 [Turkish].

in the Article 26 which is the broadest article covers the right of Freedom of Expression. The said right is regulated in the section of 'political rights and duties', rather than the section on 'personal rights and duties', unlike the rights constitute the Freedom of Expression within the Constitution. According to Article 74 of the Constitution, 'everyone has a right to ... information'. The text of the related article does not regulate any reasons for limitation of the right and it is envisaged that the limitations to be regulated by code laws, where it is stated in the last paragraph of the article with expression 'the way of exercising the rights listed in this article ... is regulated by law'.[2050]

Regulations regarding the right to information in Turkey were established with the 'Right to Information Act' numbered 4982 and published in the Official Gazette dated 24 October 2003 and numbered 25269 and with the related 'Regulation on Principles and Procedures for the Implementation of the Right to Information Act' published in the Official Gazette dated 27 April 2004 and numbered 25445.

The right to information puts public legal entities under the obligation of meeting the requests of individuals for information and documents requested in writing within legal limits that are mainly regulated with the Act and Regulation stated above. Therefore, natural and legal persons subjected to private law provisions are not legally obliged to grant the right to information to individuals. According to the letter and spirit of the Act, individuals' right to information is the priority, and the administration's obligation to provide information askes is a result of this right. With Act No. 4982, administrations, whose primary task is to carry out certain public services, are also given the duty to meet individuals' requests to information.

The purpose of the 'Right to Information Act' is to regulate the principles and procedures regarding the exercise individuals' right to obtain information from public institutions as well as professional organisations with public institution status in accordance with the principles of 'equality', 'impartiality' and 'openness' required from a democratic and transparent government. However, it should be noted that apart from the principles contained in the text of the law, the regulations in the Constitution and the European Convention on Human Rights constitute the scope of the Right to Information.

The principle of 'equality' and 'impartiality' states that the relevant administration is obliged to treat all individuals equally and impartially as a result of the application for information. The administration is obliged to provide

[2050] Dr. Karan, Ulaş, Freedom of Expression, Manuals Series for Individual Application to the Constitutional Court – 2 (European Council, 2018).

information within the scope of the relevant law to all those who exercise their right to information without making any ideological, ethnic or hierarchical discriminations. Another principle that nurtures the right to information is the principle of 'openness'. The right to information is essential for a transparent government. 'Openness' is a powerful tool for control at the hands of the person who wants to use it.[2051]

Also, it is important to mention that Article 4 of the Act states that 'everyone' has the right to obtain information in paragraph I, however; the restrictions regulated for foreigners in the paragraph II of the Article stating that they should be Turkish residents (for foreign natural persons) and engage in commercial activities in Turkey (for foreign legal entities), that the information or documents they seek should be related to their fields of activity, and that the governments of their citizenship should comply with the principle of reciprocity shows that the term 'everyone' comprises not a vast group of individuals but rather the citizens of the Republic of Turkey, as well as natural or legal persons that hold close relations to Turkey.

Confidential information or documents which will explicitly harm the State's security, external relations, national defence and national security if disclosed, are outside the scope of the right to information (Article 27 of the Regulation). Information or documents that will harm the country's economic interests or that will cause unfair competition and profits if it is disclosed or announced prematurely (Article 28 of the Regulation) are also excluded from the scope of the right to information.

Information or documents regarding the duties and activities of civil and military intelligence units are outside the scope of the right to information. However, if related information and documents affect the working life and professional dignity of individuals, information and documents related to intelligence are subjected to the right to information within the procedures and principles of the Regulation.

[2051] Cemil Kaya, *İdare Hukukunda Bilgi Edinme Hakkı* (Seçkin Yayınları, 2005) page 29 [Turkish].

9. Has your country reached an adequate balance between allowing Freedom of Expression online and protecting other rights? If not, what needs to be done to reach such balance?

9.1. Introduction

As this question merely concerns the proper balance between the allowance of Freedom of Expression online and the protection of other rights, the following answer is limited to cases where adjudicators endeavoured to strike a fair balance between the conflicting rights of different persons. In other words, cases with regard to limitations due to 'public' reasons,[2052] such as those concerning interferences based on national security or terror-related charges, are excluded from this section, akin to cases where no other individual's right was in conflict with the Freedom of Expression online.

In order to answer the question whether Turkey 'has reached' an adequate balance between Freedom of Expression online and the protection of other rights, the examination of the ECtHR jurisprudence seems undoubtedly vital in addition to the scrutiny of Turkish court cases. Nevertheless, it should be advisable to bear in mind that, as rightfully explained by the Commissioner for Human Rights of the Council of Europe:

'Recent case law of the ECtHR is not an appropriate indicator of the current situation regarding Freedom of Expression in Turkey, given the time it takes for infringements to be challenged before domestic courts, including the Constitutional Court, before bringing a case to Strasbourg.'[2053]

Nevertheless, in order to understand at least the trend occurring in the last years, relatively recent case law regarding the sought-after balance will be examined.

[2052] Dominika Bychawska, *Protecting the Right to Freedom of Expression Under the European Convention on Human Rights: A handbook for legal practitioners*, (Council of Europe 2017) 47ff; Examples can be found in many of the cases against Turkey, including 'separatist propaganda' or the question of federalisation, raised orally or in writing, have been matters of public interest. Furthermore, this section also excludes internet ban cases where access to websites were blocked under a law that prohibited 'insulting the memory of Atatürk'. (For instance, see*, Cengiz and Others v. Turkey*, App. n. 48226/10 and 14027/11, ECHR [2015]; *Akdeniz v. Turkey*, App. n. 20877/10, ECHR [2014]; *Ahmet Yıldırım v. Turkey*, App. n. 3111/10, ECHR [2012]). Differently than cases related to the conflict between Freedom of Expression online and the protection of dignity, 'the memory of Atatürk' – the founding father of the Republic of Turkey – should be deemed an issue of public interest rather than an individual right. Thus, this section does not deal with cases in respect thereof.

[2053] Commissioner for Human Rights of the Council of Europe, *Memorandum on Freedom of Expression and media freedom in Turkey (CommDH(2017)5)* (Council of Europe 2017) para 14.

9.2. ECtHR-compliant interpretation on balancing Freedom of Expression online with other rights

It should be reiterated in the first place that as to the proper balance between Freedom of Expression online and the protection of other rights, Article 90 of the Constitution of the Republic of Turkey constitutes an interpretation tool of utmost importance whereby it is stated that 'in the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail.'

It is noteworthy that Article 90 of the Turkish Constitution, not only favours the application of norms of international agreements,[2054] but it also implies the necessity of an interpretation in favour of these latter.[2055] In other words, as noted by the Turkish Constitutional Court, should a domestic provision of law be in contradiction with the ECtHR jurisprudence on the interpretation of a certain ECHR Article, the case should be resolved in accordance with Article 90 of the Constitution.[2056] Such approach was illustrated in case Adalet Mehtap Buluryer, where the Turkish Constitutional Court found that overlooking ECtHR jurisprudence in Turkish Law violated the right to a fair trial of the applicant. [2057]

9.3. Case law concerning the balance between allowing Freedom of Expression online and protecting other rights

So far, Turkish domestic courts has dealt with various Freedom of Expression online cases, particularly concerning the language and photos used in social media and their interaction with various other protected rights - *inter alia*, honour and dignity, protection of personal data, right to be forgotten, reputation and corporate identity of private law legal entities and rights of the employers to terminate the employment contract. Important decisions of the Turkish court will be examined below.

2054 *Sevim Akat Eşki*, App. n. 2013/2187, Constitutional Court of the Republic of Turkey [2013] 41; *Adalet Mehtap Buluryer Kararı*, App. n. 2013/5447, Constitutional Court of the Republic of Turkey [2014] 46 [Turkish].

2055 Ulaş Karan, Freedom of Expression, Manuals Series for Individual Application to the Constitutional Court – 2, European Council [2018] 129 [Turkish].

2056 *Adalet Mehtap Buluryer Kararı*, App. n. 2013/5447, Constitutional Court of the Republic of Turkey [2014] 52–53 [Turkish].

2057 *Adalet Mehtap Buluryer Kararı*, App. n. 2013/5447, Constitutional Court of the Republic of Turkey [2014] 52–53 [Turkish].

9.4. Freedom of Expression online and the right to be forgotten

The case of N.B.B.[2058] concerned a Turkish citizen (N.B.B.) who was convicted of drug related crimes in 1998. Between 1998 and 1999, a national newspaper published three articles about his conviction which were subsequently added to an online archive. In 2013, alleging that they were outdated and harmed his reputation, N.B.B. requested that the newspaper de-index the articles. The Constitutional Court found that the articles were outdated, served no public interest purpose, and that making them publicly available online harmed N.B.B. 's reputation.

The case of N.B.B constitutes a landmark decision since the Court examined multiple factors in determining whether the Right to Freedom of Expression can be outweighed by the 'Right to be Forgotten', including: the content of the news; the time period of publication of the news; whether the news is up-to-date or whether the news can be accepted as historical information; whether the news contribute to the public welfare; whether the person subject to the news is a political or social figure; whether there are value judgment or facts in the content of the news; and the level of interest of the public towards the news.[2059]

At the case in hand, even though the articles did not contain any false information, the Court held that they no longer could be deemed relevant or up to date, neither they contained any statistical or scientific information which would justify their availability to the public. Thus, the Court found that the articles violated the N.B.B.'s 'right to be forgotten'.

9.5. Use of images and limitations on the Freedom of Expression online

According to the jurisprudence of the European Court of Human Rights publication of photos also falls into the ambit of Freedom of Expression, nevertheless, this is an area 'in which the protection of the rights and reputation of others takes on particular importance, as the photos may contain very personal or even intimate information about an individual or his or her family

---

2058 *N.B.B. Başvurusu*, *App. n. 2013/5653,* Constitutional Court of the Republic of Turkey [2016] [Turkish].

2059 Columbia University, 'Global Freedom of Expression, *The Case of N.B.B.'* <https://globalfreedomofexpression.columbia.edu/cases/case-n-b-b/> accessed 21 February 2020; The approach of the Turkish Constitutional Court may be deemed compatible with the ECtHR jurisprudence as in order to balance the right to Freedom of Expression against the right to private life. The ECtHR uses six criteria established fundamentally in the case of *Axel Springer AG v. Germany* the contribution to a debate of general interest; how well known the person being reported on is and the subject of the report; the person's prior conduct; the method used to obtain the information; the veracity, content, form and repercussions of the report; and the penalty imposed. See, (*Axel Springer AG v. Germany* [GC], no. 39954/08, [2012]).

…'[2060] Turkish domestic courts have been active in dealing with questions related to this sensitive area.

In decision E. 2012/2015 K. 2014/331[2061], Plenary Assembly of the Penal Department no 12 of the Supreme Court ('Penal Department') dealt with the question whether using other individuals' photos in social media constitute a limitation to the Freedom of Expression. The case concerned a woman who worked as the editor-in-chief of a domestic journal who used a photo of an employee of the same journal as her profile photo at a dating website. The Penal Department found that such a use of photos of other individuals constituted the crime of disseminating personal data unlawfully, and also of public defamation pursuant to the first and fourth paragraph of Article 125 of the Turkish Criminal Code, as it may violate the honour and dignity of the individual whose photo is used.

However, Turkish case law does not seem to be consistent in respect of personal data protection in cases of use of photos in social media. In this regard, particular attention should be given to the decision E. 2015/4349 K. 2016/5349 of the 12th Chamber of the Penal Department.[2062] In the case, the accused who used a fake profile published the Facebook profile picture of the complainant, which was publicly visible, put differently, not exclusively visible to those in his/her friends list. The Penal Department found that it is not a crime to publish, without using the name and surname of the person concerned, photos that are not related to private life and are easily obtained from a public Facebook profile.[2063] However, this does not necessarily mean that such publications should be immune to any claims per se and deemed to fall in the ambit of the freedom expression online. In fact, even though the Penal Department decided that no criminal liability should occur for the accused, at the end of its decision, it added that these actions can be subject to private law sanctions.

[2060] Peck v. the United Kingdom, no. 44647/98, 28 [2003]; Reklos and Davourlis v. Greece, no. 1234/05, [2009]; Société de Conception de Presse et d'Edition v. France, no. 4683/1, ECHR [2016]; Bogomolova v. Russia, no. 13812/09, [2017].

[2061] App. n. 2012/2015 Constitutional Court of the Republic of Turkey [2014] [Turkish].

[2062] App. n. 2015/4349 Penal Department No. 12 of the Supreme Court [2016] [Turkish].

[2063] In this regard, distinction should be made between cases concerning the use of publicly available photos and those concerning the publication of unconsentedly taken photos examined under Articles 8 and 10 of the ECHR. (For instance, *Kahn v. Germany*, *App. n. 16313/10* ECHR [2016].

9.6. Freedom of Expression online and copyright legislation

According to the jurisprudence of ECtHR Freedom of Expression also includes access to information.[2064] The case *Akdeniz v. Turkey*[2065] concerned the complaint of Mr. Yaman Akdeniz in particular of a violation of his Freedom of Expression as access to two music-streaming websites was blocked by the media division of the public prosecutor's office on the ground that they had streamed music without respecting copyright legislation. Mr. Akdeniz lodged appeals against the measure in question which were dismissed by the lower and higher criminal courts, respectively. The courts, finding that the applicant could not be considered a 'victim', held that the blocking measure had been based on Law no. 5846 on artistic and intellectual works and had been adopted on account of the copyright infringements of the websites in question. Akin to the Turkish domestic courts, the application was found to be inadmissible (incompatible *ratione personae*) by the ECtHR, declaring that the applicant did not have 'victim' status in terms of Article 34 of the Convention. Furthermore, while underlining the utmost importance of the rights of internet users, the Court added that the block was due to the breach of copyright law and that as a user of these websites, the applicant had lost merely one method of listening to music amongst many others.

9.7. Freedom of Expression online and honour, dignity and reputation of persons

In contrast to some relatively older cases which subsequently led to violations of Article 10 of ECtHR[2066], a gradation of protection for different groups can be seen from the recent jurisprudence of the Turkish Constitutional Court in

[2064] Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes v. Austria no. 39534/07 ECHR [2013] 41.

[2065] *Akdeniz v. Turkey*, App. n. 20877/10 ECHR [2014].

[2066] See for instance, *Erdoğan v Turkey*, App. n. 39656/03 ECHR [2009] where the applicant, a practising lawyer, in a written submission to the Istanbul Administrative Court, referred to the mayor as a cruel person and a bigot with no regard for the rule of law. The mayor's office in turn brought an action against Erdoğan for the damage he had allegedly incurred as a result of the applicant's attack on his honour and integrity. The domestic court found in favour of the mayor and ordered Erdoğan to pay a significant sum of compensation. Subsequently, the ECtHR held that Erdoğan's remarks could not be construed as a gratuitous personal attack in the context of judicial proceedings in which he was acting in his capacity as a legal representative. Although the Court held that Erdoğan's comments were clearly of a nature to discredit the mayor, it reiterated that the mayor was not a private individual but a public figure. Moreover the negative impact of Erdoğan's words on the mayor's reputation would be limited, since they were confined to a courtroom rather than, for example, being voiced to the media.

parallel with that of the ECtHR.[2067] In the case of Ali Rıza Üçer,[2068] applicant Mr. Üçer authored an article which was published online by an association of which he was a member. In the article, Mr. Üçer concluded that the drinking water provided by the Ankara Metropolitan Municipality contained cancerogenic materials. The Metropolitan Municipality mayor brought an action against Mr. Üçer claiming that he was 'insulted and humiliated'. Finding the mayor's claims right, the court of first instance entitled him to compensation. Underlining the broader protection applicable to the criticism of particularly public figures and politicians, The Constitutional Court held that Mr. Üçer's Freedom of Expression was violated by the sanction of compensation.

In the case of *Orhan Pala*,[2069] the applicant was a journalist and the chief editor of a stock exchange website who published at the latter a report about the shareholders of a number of companies whose shares were traded on the Istanbul Stock Exchange (ISE). According to the report in question, the complainants had been tried and convicted of manipulation in the past, but the conviction was not finalised due to the limitation of action. The rest of the report gave information about the companies recently bought by the shareholders and questioned the source of these latter's wealth as allegedly they were living in luxury. The report resulted in a sudden and unexpected decrease in the shares of the company belonging to the shareholders in question. Claiming that the information in the report was false, and that it damaged their reputation and decreased their shares unjustly, the shareholders filed a criminal complaint against the applicant. The court of first instance sentenced the applicant to two months and 27 days in prison based on defamation but deferred the announcement of the verdict.

While noting that 'malicious distortions of reality can sometimes exceed acceptable limits of criticism', the Constitutional Court stated that 'waiting for journalists to act like a prosecutor responsible for proving the accuracy of a statement would mean an extremely high burden of proof.' According to the Court, the conditions to be taken into account while determining the degree of the obligation to investigate the correctness of factual statements that are claimed to be insulting about private individuals are:

2067 Dominika Bychawska, Protecting the Right to Freedom of Expression Under the European Convention on Human Rights: A handbook for legal practitioners, (Council of Europe 2017) 63; See for instance, *Lingens v. Avusturya*, no. 9815/82, 08.07.1986, 42.

2068 *Ali Rıza Üçer Başvurusu, App. n. 2013/8598* Constitutional Court of the Republic of Turkey [2016] [Turkish] 56.

2069 *Orhan Pala Başvurusu, App. n. 2014/2983* Constitutional Court of the Republic of Turkey [2017] [Turkish].

— The nature and degree of the factual statement in question;

— Whether the news sources are reasonably reliable in terms of such claims; and

— Whether journalists act in good faith to provide accurate and reliable information.

— Infringement of public peace

The Constitutional Court found that the applicant Mr. Pala acted responsibly enough as a journalist and his Freedom of Expression – as well as press – online was violated.

The Constitutional Court took a very similar approach in case *Medya Gündem*[2070] which concerned an online publication analysing the changes in the free float of a Company, as well as the increases and decreases in its shares from the time it entered the stock market until the date of publication. Stressing that the claims and evaluations regarding the Company whose shares are offered to the public are statements that are of public interest, The Constitutional Court found that eliminating without any justification the possibility of spreading opinions that concern the public means 'censorship' and it concluded that the interference with the applicant's Freedom of Expression online did not constitute a necessary intervention in the democratic social order to protect the reputation and rights of others.

In another case,[2071] the Penal Department No 9 held that the acceptable limits of criticism were exceeded where a bank employee used the expression '… it is not a bank of justice distribution because it has only been the bank of the privileged and tag tails' in social media for the bank he was working at. The Penal Department No 9 found that such an expression was humiliating and able to violate the reputation and the corporate identity of the bank.

9.8. Conclusion

In sum, it may be reasonable to conclude that, while there might be some exceptional cases, Turkish Courts have not failed in striking an adequate balance between Freedom of Expression online and the protection of other rights. It may also be observed that this is mainly due to the decisions of the Constitutional Court, where ECtHR jurisprudence was followed as an example. With respect to the balance between Freedom of Expression online and other

[2070] *Medya Gündem Dijital Yayıncılık Ticaret A.Ş.* [2013] Constitutional Court of the Republic of Turkey 2623 [2015] [Turkish].

[2071] App. n. 2014/11621 Penal Department No. 9 of the Supreme Court [2014] [Turkish].

rights of private individuals it seems indeed difficult to find a recent case where Turkish Courts made an interpretation in a non-ECHR-compliant manner.[2072] However, as mentioned above, this conclusion is made solely for the cases where the balance was sought after between the conflicting rights of different persons. The adequacy of Turkey's interference in the Freedom of Expression online in respect of cases concerning limitations due to public reasons, such as national security, territorial integrity or terror-related charges, will be examined at the further sections of this report.

10. How do you rank the access to Freedom of Expression online in your country?

In light of the explanations above, our ranking regarding the access to Freedom of Expression online in Turkey would be 2 out of 5, considering the web accessibility (10.1), limits on content (10.2) and violations of user rights (10.3) in recent years.

10.1 Access to Internet

Internet access is not restricted directly by infrastructural limitations or the speed and quality of internet connections. Also, the internet penetration rates are on the rise. According to the results of the Turkish Statistical Institute's Household Usage of Information Technologies Survey, the rate of households with internet access had risen to 88.3 percent in 2019, compared to 83.8 percent in 2018. However, in past years, connectivity in the south-eastern region was negatively affected by poor telecommunications infrastructure and electricity blackouts. On certain occasions, social media platforms and private messaging applications are throttled to limit online communications in the aftermath of terrorist attacks, security and military-related incidents.

[2072] See for instance, 'The Commissioner and his predecessor had observed in previous reports that prosecutors and courts in Turkey often perceive dissent and criticism as a threat to the integrity of the state, and see their primary role as protecting the interests of the state, as opposed to upholding the human rights of individuals. Particular concerns relating to Freedom of Expression have been the use of the concept of 'incitement to violence', which was systematically interpreted in a non-ECHR-compliant manner.' Commissioner for Human Rights of the Council of Europe, Memorandum on Freedom of Expression and media freedom in Turkey (CommDH(2017)5) (Council of Europe 2017) para 8; See also, for the previous report, Commissioner for Human Rights of the Council of Europe, Freedom of Expression and media freedom in Turkey (Report by Thomas Hammarberg) (CommDH(2011)25) (Council of Europe 2011).

10.2 Limits on Content

Blocking of online content, particularly news and citizen journalism websites, has increased in recent years. Engelli Web[2073], a civil society initiative that lists blocked websites in Turkey, found that more than 240 thousand websites were inaccessible as of December 2018, while it was about 40 thousand in 2013. Websites can be blocked for grounds such as 'obscenity' or content that is defamatory to Islam and promotes atheism.[2074] However, the increase in censored content in recent years is largely due to the blocking of news sites and articles that are critical of the government. According to Engelli Web, over 3 thousand URLs containing news items were blocked in 2018.

In addition to widespread filtering, state authorities are proactive in requesting the deletion or removal of content. Social media platforms comply with administrative decisions and court orders promptly in order to avoid blocking and, more recently, throttling. Like international social media platforms, popular Turkish websites are subject to content removal orders.

Turkey has consistently ranked among the countries with the highest number of removal requests sent to Twitter. According to Twitter's latest transparency report, between January and June 2019, the Turkish government made over 6 thousand removal requests, and Twitter complied with five percent of them. In the second half of 2018, the government made over 5 thousand removal requests, and Twitter complied with four percent of them. [2075]

Facebook and Instagram also received a large number of content restriction requests from Turkey. According to Facebook's transparency report covering January to June 2019, 251 pieces of content were restricted by Facebook, which covers a range of offenses including personal rights violations, personal privacy, defamation of Atatürk, and laws on the unauthorised sale of regulated goods, and 348 items in response to private reports of defamation. Between January and June 2018, 1,634 pieces of content were restricted, 1,106 at the request of the government, and 528 in response to private reports of defamation.[2076] Some analysts believe the declining number of requests can be attributed to the government's shift to blocking content through technical means.

2073 Yaman Akdeniz and Ozan Guven, '*Engelli Web 2018'* (July 2019) <https://ifade.org.tr/reports/EngelliWeb_2018_Eng.pdf> accessed 12 February 2020 [Turkish].

2074 Efe Kerem Sözeri*, 'Turkey quietly escalating online censorship of atheism',* The Daily Dot, March 4, 2015 <https://www.dailydot.com/layer8/turkey-secret-ban-atheist-content/> accessed 20 May 2020.

2075 Twitter, *'Transparency Report – Removal Requests, Turkey' (*February 2020) <https://transparency.twitter.com/en/removal-requests.html> accessed 10 February 2020.

2076 Facebook, *'Transparency Report, Turkey'* <https://transparency.facebook.com/content-restrictions/country/TR> accessed 10 February 2020.

Many of the restrictions on the internet and digital content lack proportionality and transparency. The blocking and removal of online content is regulated under Law No. 5651. The responsibilities of content providers, hosting companies, public access providers, and internet service providers (ISPs) are delineated in this law. Domestically hosted websites with proscribed content can be taken down, while websites based abroad can be blocked and filtered through ISPs.

The majority of blocking orders are issued by the BTK, rather than by the courts. The procedures surrounding blocking decisions are not transparent, creating significant challenges for those seeking to appeal. The reasoning behind court decisions is not provided in blocking notices, and the relevant rulings are not easily accessible. As a result, it is often difficult for site owners to determine why their site has been blocked and which court has issued the order. The BTK's mandate includes executing judicial blocking orders, but it can also issue administrative orders for foreign websites, content involving sexual abuse of children, and obscenity. Moreover, in some cases it successfully asks content and hosting providers to remove offending items from their servers, in order to avoid issuing a blocking order that would affect an entire website. This occurs despite the fact that intermediaries are not responsible for third-party content on their sites.

Freedom of Expression online is inhibited by heightened self-censorship. A steep rise in prosecutions for defaming the president has also had a chilling effect on social media users in recent years. Self-censorship online has been exacerbated by decrees passed under the state of emergency that have expanded surveillance.

10.3 Violations of user rights

The constitution and laws of Turkey fall short of protecting Freedom of Expression and press freedom online. According to the Council of Europe Commissioner's Memorandum of 2017, the legislation 'needs to be reviewed completely in order to make it ECHR-compliant.'[2077] Turkish citizens faced investigations and arrests for their online activities. The state of emergency enacted in the wake of the 2016 coup attempt and stayed in effect until July 2018 allowed the President to issue decrees without judicial oversight, including decrees that threatened Freedom of Expression online, which were used to block websites, shut down communication networks, and close civil society organisations and news outlets. Decree No. 671, published in 2016, amended the Law on Digital Communications to authorise the government to take 'any

[2077] Commissioner for Human Rights of the Council of Europe, *Memorandum on Freedom of Expression and media freedom in Turkey* (CommDH(2017)5) (Council of Europe 2017).

necessary measure' on the grounds of 'national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms' guaranteed under Article 22 of the constitution. The decree also obliges telecommunications providers to enforce government orders within two hours of receiving them. Despite the fact that the state of the emergency is no longer in effect, the decree remains on the books.

Prosecutions for insulting the president online have increased in recent years, although they have rarely resulted in convictions. However, some defendants have been jailed while awaiting trial. Insulting the president online is an offense punishable by up to four years in prison.

Thus, the accusations raised by the European Commission in recent years – namely that Turkish law is not able to guarantee a level of Freedom of Expression as demanded by the European Convention on Human Rights (ECHR) and the European Court of Human Rights (ECtHR) remain true. In its Freedom on the Net 2019 report, Freedom House ranks Turkey once again as 'Not Free' stating that between June 2018 and May 2019 online content was frequently blocked, including news articles, and authorities continued to investigate or arrest users.[2078] As to Bertelsmann Transformation Index (BTI), the tendency to curtail Freedom of Expression observable between 2012 and 2014 continued and Turkey's ranking on Freedom of Expression diminished to 4 points out of 10, particularly after the failed military coup attempt in 2016.[2079]

11. How do you overall assess the legal situation in your country regarding internet censorship?

Turkey joined the Internet in the 1990s. Today, internet access rates are high in Turkey, and it is an essential part of people's lives. In the Turkish Statistical Institute's Household Usage of Information Technologies Survey, it is reported that internet access rate among households had increased to 83.8 percent in 2018.[2080]

2078 Freedom House, *'Freedom on the Net 2019'* <https://www.freedomonthenet.org/country/turkey/freedom-on-the-net/2019> accessed 10 February 2020.

2079 Bertelsmann Stiftung, *'BTI 2018 Country Report — Turkey' Gütersloh'*, Bertelsmann Stiftung, 2018 <https://www.bti-project.org/fileadmin/files/BTI/Downloads/Reports/2018/pdf/BTI_2018_Turkey.pdf> accessed 10 February 2020.

2080 *'TURKSTAT News Bulletin' (No: 27819, 08 August 2018)*, <http://www.tuik.gov.tr/PreHaberBultenleri.do?id=27819 >, accessed 23 May 2020.

As the Internet became popular in today's society, regulations on the Internet improved too. The Convention on Cybercrime also known as the Budapest Convention is the first international treaty dealing with computer crime and internet which ratified by Turkish parliament in 2014.

In Turkey, regulations developed after Law No. 5651, which was entered into force on the 23 May 2007, upon its publication in the Official Gazette which is named On Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication known also as the Internet Law.

According to Law No 5651, access to an Internet site may be blocked by a judge of the peace or where a delay would present a risk, by The Information and Communication Technologies Authority (BTK). The BTK was responsible for approximately 95 percent of the websites blocked in 2018. [2081]

On the face of it, in upcoming years Turkey will have more censorship with this regulations, easy sensor mechanism by public enterprise as the Supreme Council of Radio and Television (RTUK) and BTK (before, TIB) and projects as *Güvenli İnternet* (secure usage of Internet).

Internet Law is a new regulation for internet services. In 2018, the Turkish parliament passed a law authorising the national broadcast media regulator, the Supreme Council of Radio and Television (RTUK) to monitors and regulates internet services and makes online video and streaming services necessary to apply for a license. According to the decision published in the Official Gazette on 1 August 2019, which named Regulation on the Web-Based Presentation of Radio and Television Broadcasts and Video On-Demand Services, online media service providers such as Netflix and BluTV, came under the control of the Supreme Council of Radio and Television (RTUK).

In the last decade, Twitter, YouTube, Wikipedia, and more banned by Turkish authorisations. In the last years, laws on blocking IP number or domain name negatively affect people in Turkey regarding freedom speech. In this context, popular social media platforms such as YouTube and Twitter have been blocked at all due to a video and post instead of blocking related content.

In recent years, blocking of online content has increased. According to Engelli Web which is a civil society organisation that lists blocked websites in Turkey, determined more than 245,825 websites were inaccessible by the end of 2018. However, the increase in censored content in recent years is largely due to the

[2081] Yaman Akdeniz and Ozan Guven, *'Engelli Web 2018'* (July 2019) <https://ifade.org.tr/reports/EngelliWeb_2018_Eng.pdf >, accessed 23 May 2020 [Turkish].

blocking of news sites and articles that are critical of the government. According to Engelli Web, 3,306 URLs containing news items were blocked in 2018.[2082]

According to Freedom on the Net Report 2019, Turkey is reported 'Not Free' from June 2018 to May 2019 period one more time due to some reasons such as frequently blocked or continued to investigate authorities. [2083]

Currently, constitutional safeguards of Freedom of Expression are only partially covered in practice. They are generally undermined by provisions Law No. 5651 (Internet Law). Although Turkey has strongly ensured Freedom of Expression by the Constitution and legislation, the public enterprises practice law as a censorship machine. This illegal situation is criticised by domestic and foreign sources in Turkey.

[2082] Yaman Akdeniz and Ozan Guven, *'Engelli Web 2018'* (July 2019) <https://ifade.org.tr/reports/EngelliWeb_2018_Eng.pdf>, accessed in 21 May 2020 [Turkish].

[2083] Adrian Shahbaz and Allie Funk, Freedom House*, 'Freedom on the Net 2019'* <https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf >, accessed 21 May 2020.

Conclusion

Turkey has been reported to have nearly 62 million internet users and 54 million social media users by January 2020 according to DataReportal's Digital 2020 report. While having a large number of internet users the Turkey has faced with many issues regarding Freedom of Expression online.

In the recent years, the Turkish government made amendments to the Internet Law and adopted new regulations which led to increase in restrictions on internet freedom. The enacted laws have expanded both the state's control on blocking websites and the surveillance capability of the government. Also, the extent of these limitations has likewise been extended and therefore increased the number of indicted individuals and self-censorship among community.

Furthermore, internet freedom in Turkey was categorised as 'not free' by the Freedom House. This is a result of increasing numbers of limits on content and violation of user rights.

Hence it can be concluded, Freedom of Expression is one of the fundamental human rights and is protected by The European Convention on Human Rights. However, currently, constitutional guarantees of Freedom of Expression online are only partially upheld in practice.

Table of legislation

Title of the legal act	**Provision text in English language**
Constitution of the Republic of Turkey, Article 13	(As amended on October 3, 2001; Act No. 4709) Fundamental rights and freedoms may be restricted only by law and in conformity with the reasons mentioned in the relevant articles of the Constitution without infringing upon their essence. These restrictions shall not be contrary to the letter and spirit of the Constitution and the requirements of the democratic order of the society and the secular republic and the principle of proportionality.
Constitution of the Republic of Turkey, Article 14	(As amended on October 3, 2001; Act No.4709) None of the rights and freedoms embodied in the Constitution shall be exercised in the form of activities aiming to violate the indivisible integrity of the State with its territory and nation, and to endanger the existence of the democratic and secular order of the Republic based on human rights. No provision of this Constitution shall be interpreted in a manner that enables the State or individuals to destroy the fundamental rights and freedoms recognised by the Constitution or to stage an activity with the aim of restricting them more extensively than stated in the Constitution. The sanctions to be applied against those who perpetrate activities contrary to these provisions shall be determined by law.
Constitution of the Republic of Turkey, Article 15	(As amended on April 16, 2017; Act No. 6771) In times of war, mobilisation, a state of emergency, the exercise of fundamental rights and freedoms may be partially or entirely suspended, or measures derogating the guarantees embodied in the Constitution may be taken to the extent required by the exigencies of the situation, as long as obligations under international law are not violated. (As amended on May 7, 2004; Act No. 5170) Even under the circumstances indicated in the first paragraph, the individual's right to life, the integrity of his/her corporeal and spiritual existence shall be inviolable except where death occurs through acts in conformity with law of war; no one shall be compelled to reveal his/her religion, conscience, thought or opinion, nor be accused on account of them; offences and penalties shall not be made retroactive; nor shall anyone be held guilty until so proven by a court ruling.
Constitution of the Republic of Turkey, Article 20/3	Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law.

Constitution of the Republic of Turkey, Article 26	Everyone has the right to express and disseminate his/her thoughts and opinions by speech, in writing or in pictures or through other media, individually or collectively. This freedom includes the liberty of receiving or imparting information or ideas without interference by official authorities. This provision shall not preclude subjecting transmission by radio, television, cinema, or similar means to a system of licensing. The exercise of these freedoms may be restricted for the purposes of national security, public order, public safety, safeguarding the basic characteristics of the Republic and the indivisible integrity of the State with its territory and nation, preventing crime, punishing offenders, withholding information duly classified as a state secret, protecting the reputation or rights and private and family life of others, or protecting professional secrets as prescribed by law, or ensuring the proper functioning of the judiciary. (Repealed on October 3, 2001; Act No. 4709) Regulatory provisions concerning the use of means to disseminate information and thoughts shall not be deemed as the restriction of Freedom of Expression and dissemination of thoughts as long as the transmission of information and thoughts is not prevented. (Paragraph added on October 3, 2001; Act No. 4709) The formalities, conditions and procedures to be applied in exercising the Freedom of Expression and dissemination of thought shall be prescribed by law.
Constitution of the Republic of Turkey, Article 28	The press is free and shall not be censored. The establishment of a printing house shall not be subject to prior permission or the deposit of a financial guarantee. (Repealed on October 3, 2001; Act No. 4709) The State shall take the necessary measures to ensure freedom of the press and information. In the limitation of freedom of the press, the provisions of articles 26 and 27 of the Constitution shall apply. Anyone who writes any news or articles which threaten the internal or external security of the State or the indivisible integrity of the State with its territory and nation, which tend to incite offence, riot or insurrection, or which refer to classified state secrets or has them printed, and anyone who prints or transmits such news or articles to others for the purposes above, shall be held responsible under the law relevant to these offences. Distribution may be prevented as a precautionary measure by the decision of a judge, or in case delay is deemed prejudicial, by the competent authority explicitly designated by law. The authority preventing the distribution shall notify a competent judge of its decision within twenty-four hours at the latest. The order preventing distribution shall become null and void unless upheld by a competent judge within forty-eight hours at the latest. No ban shall be placed on the reporting of events, except by the decision of judge issued within the limits specified by law, to ensure proper functioning of the judiciary. Periodical and non-periodical publications may be seized by a decision of a judge in cases of ongoing investigation or prosecution of crimes specified by law; or by order of the competent authority explicitly designated by law, in situations where delay may constitute a prejudice with

	respect to the protection of the indivisible integrity of the State with its territory and nation, national security, public order or public morals and for the prevention of crime. The competent authority issuing the order to seize shall notify a competent judge of its decision within twenty-four hours at the latest; the order to seize shall become null and void unless upheld by a judge within forty-eight hours at the latest. General provisions shall apply when seizing and confiscating periodicals and nonperiodicals for reasons of criminal investigation and prosecution. Periodicals published in Turkey may be temporarily suspended by court ruling if found to contain material which contravenes the indivisible integrity of the State with its territory and nation, the fundamental principles of the Republic, national security and public morals. Any publication which clearly bears the characteristics of being a continuation of a suspended periodical is prohibited; and shall be seized by decision of a judge.
Constitution of the Republic of Turkey, Article 32	The right of rectification and reply shall be accorded only in cases where personal reputation and honor is injured or in case of publications of unfounded allegation and shall be regulated by law. If a rectification or reply is not published, the judge decides, within seven days of appeal by the individual involved, whether or not this publication is required. XI. Rights and freedoms of assembly
Constitution of the Republic of Turkey, Article 90	The ratification of treaties concluded with foreign states and international organisations on behalf of the Republic of Turkey shall be subject to adoption by the Grand National Assembly of Turkey by a law approving the ratification. Agreements regulating economic, commercial or technical relations, and covering a period of no more than one year, may be put into effect through promulgation, provided they do not entail any financial commitment by the State, and provided they do not interfere with the status of individuals or with the property rights of Turks abroad. In such cases, these agreements shall be brought to the knowledge of the Grand National Assembly of Turkey within two months of their promulgation. Implementation agreements based on an international treaty, and economic, commercial, technical, or administrative agreements, which are concluded depending on the authorisation as stated in the law, shall not require approval of the Grand National Assembly of Turkey. However, economic, commercial agreements or agreements relating to the rights of individuals concluded under the provision of this paragraph shall not be put into effect unless promulgated. Agreements resulting in amendments to Turkish laws shall be subject to the provisions of the first paragraph. International agreements duly put into effect have the force of law. No appeal to the Constitutional Court shall be made with regard to these agreements, on the grounds that they are unconstitutional. (Sentence added on May 7, 2004; Act No. 5170) In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to

	differences in provisions on the same matter, the provisions of international agreements shall prevail.
Turkish Criminal Code Article 84	(1) Any person who solicits, encourages a person to commit suicide, or supports the decision of a person for suicide or helps the suicide action in any manner whatsoever, is punished with imprisonment from two years to five years. (2) In case of commission of suicide, the person who is involved in such act is sentenced to imprisonment from four years to ten years. (3) Any person who openly encourages others to commit suicide is punished with imprisonment from three years to eight years. (5) Persons who encourage others, lack of ability to understand the meaning and consequences of the executed act, to commit suicide, or force a person to commit suicide under threat, are convicted of felonious homicide.
Turkish Criminal Code Article 103/1	1) Any person who abuses a child sexually is sentenced to imprisonment from three years to eight years.
Turkish Criminal Code Article 190	(1) Any person facilitating use of addictive or relieving/exciting drugs by; a) Providing special place, equipment or material, b) Taking precautions to avoid arrest of users, c) Furnishing information to others about the method of use, is punished with imprisonment from two years to five years. (2) In case of commission of the offenses defined in this article by a physician, dentist, pharmacist, chemist, veterinary, health personnel, laboratory technician, midwife, nurse dentistry technician, or any other person rendering health service or dealing in production and trading of chemicals or in pharmacy, the punishment to be imposed is increased by one half. (3) Those who openly encourage use of addictive or exciting drugs, or makes publication with this purpose, is punished with imprisonment from two years to five years.
Turkish Criminal Code Article 194	Any person who supplies or delivers substances to children, persons suffering from mental illness or others using evaporative substances, or presents such products to consumption risking others' life, is punished to imprisonment from six months to one year.
Turkish Criminal Code Article 226	(1) Any person who involves in an unlawful act; a) By allowing a child to watch indecent scene or a product, or to or hear shameful words, b) By displaying these products at places easy to reach by children, or reading the contents of these products, or letting other to speak about them, c) By selling or leasing these products in such a way open for public review, d) By selling, offering or leasing these products at places other than the markets nominated for sale of these product, e) By gratuitously supplying or distributing these products along with other goods or services, f) By making advertisement of these products, is punished with imprisonment from six months to two years.

Article 36 of the Turkish Constitution	Citizens and foreigners resident in Turkey, with the condition of observing the principle of reciprocity, have the right to apply in writing to the competent authorities and to the Grand National Assembly of Turkey with regard to the requests and complaints concerning themselves or the public.
Article 14 of the Turkish Constitution	Everyone has the right of litigation either as plaintiff or defendant and the right to a fair trial before the courts through legitimate means and procedures. No court shall refuse to hear a case within its jurisdiction.
Article 6 of the Law n. 5651	None of the rights and freedoms embodied in the Constitution shall be exercised in the form of activities aiming to violate the indivisible integrity of the State with its territory and nation, and to endanger the existence of the democratic and secular order of the Republic based on human rights. No provision of this Constitution shall be interpreted in a manner that enables the State or individuals to destroy the fundamental rights and freedoms recognised by the Constitution or to stage an activity with the aim of restricting them more extensively than stated in the Constitution. The sanctions to be applied against those who perpetrate activities contrary to these provisions shall be determined by law.

Bibliography

English titles

Legislation

Constitution of the Republic of Turkey

Electronic Communications Law no. 5809

Law on Intellectual and Artistic Works no. 5846

Law on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts no. 5651

Regulation on the Web-Based Presentation of Radio and Television Broadcasts and Video On-Demand Services

Right to Information Act no. 4982

Turkish Criminal Code no. 5237

Turkish Commercial Code no. 6102

Turkish Law of Obligations no. 6098

Turkish Personal Data Protection Law no. 6698

Reports

Commissioner for Human Rights of the Council of Europe, Memorandum on Freedom of Expression and media freedom in Turkey (CommDH(2017)5) (Council of Europe 2017) para 111.

Eugen Chelaru and Marius Chelaru Right to be Forgotten 16 Annales Universitatis Apulensis Series Jurisprudentia 26 (2013).

European Union: European Commission, European Commission for Democracy Through Law (Venice Commission), Turkey -Law No. 5651- On Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication, 15 June 2016 , CDL-AD(2016)011, para 44.

Fostering Freedom Online: the Role Of Internet Intermediaries.

The Privacy, Data Protection and Cybersecurity (Law Review - Edition 6, The Law Reviews, October 2019).

Rebecca MacKinnon-Elonnai Hickok-Allon Bar-Hae-in Lim - United Nations Educational, Scientific and Cultural Organization (UNESCO,2014).

Books

Bülent Tanör; Necmi Yüzbaşıoğlu, Turkish Constitutional Law According to the Constitution of 1982 ('1982 Anayasası'na Göre Türk Anayasa Hukuku'), Beta Yay., İstanbul, 2006, s. 159.

Dominika Bychawska, Protecting the Right to Freedom of Expression Under the European Convention on Human Rights: A handbook for legal practitioners, (Council of Europe 2017).

Dr. Karan, Ulaş, Freedom of Expression, Manuals Series for Individual Application to the Constitutional Court – 2, European Council, 2018, page 93.

Digital resources

'Access to Wikipedia Reinstated in Turkey' <https://www.gurkaynak.av.tr/docs/5b36c-access-to-wikipedia-reinstated-in-turkey.pdf> accessed 10 February 2020.

Akdeniz Yaman and Güven Ozan, 'Engelli Web 2018' (July 2019) <https://ifade.org.tr/reports/EngelliWeb_2018_Eng.pdf> accessed 12 February 2020.

Akdeniz, Yaman. 'Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship.' OSCE , Organization for Security and Co-Operation in Europe The Representative on Freedom of the Media, < www.osce.org/fom/41091?download=true> accessed 10 May 2020.

Bertelsmann Stiftung, 'BTI 2018 Country Report — Turkey' Gütersloh: Bertelsmann Stiftung, 2018 <https://www.bti-project.org/fileadmin/files/BTI/Downloads/Reports/2018/pdf/BTI_2018_Turkey.pdf> accessed 10 February 2020.

Columbia University Global Freedom of Expression, 'The Case of N.B.B.' <https://globalfreedomofexpression.columbia.edu/cases/case-n-b-b/> accessed 21 February 2020.

'Current version of Constitution of the Republic of Turkey including latest amendments 08.05.2017' <http://www.judiciaryofturkey.gov.tr/Current-version-of--Constitution-of-the-Republic-of-Turkey--including-latest--amendments> accessed 25 May 2020.

Ergün, Fevzi Doruk. 'National Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy.' (Edam, Edam, 3 April 2018) <edam.org.tr/en/national-security-vs-online-rights-and-freedoms-in-turkey-moving-beyond-the-dichotomy/> accessed 10 May 2020.

'Everything You Need to Know About 'the Right to be Forgotten' <https://gdpr.eu/right-to-be-forgotten/ > accessed 25 May 2020.

Facebook, 'Transparency Report, Turkey' <https://transparency.facebook.com/content-restrictions/country/TR> accessed 10 February 2020.

Freedom House, 'Freedom on the Net 2019' <https://www.freedomonthenet.org/country/turkey/freedom-on-the-net/2019> accessed 10 February 2020.

Global Freedom of Expression (Columbia University) <https://globalfreedomofexpression.columbia.edu/cases/cengiz-v-turke/>accessed 21 February 2020.

Golbasi Criminal Court of Peace Decision No 2015/191 D.Is, dated February 27 2015, Efe Kerem Sözeri, 'Turkey quietly escalating online censorship of atheism,' The Daily Dot (4 March 2015)<https://www.dailydot.com/layer8/turkey-secret-ban-atheist-content/> accessed 20 May 2020.

Gürkaynak, Gönenç, and Yılmaz, İlay. 'New Access Ban Regime Proposed for Law 5651.'(Globe Business Media Group, 24 Mar. 2015) <www.gurkaynak.av.tr/docs/New-access-ban-regime-proposed-for-Law-5651.pdf.> accessed 10 May 2020.

'Intermediary Liability Updates from Turkey: Forcing Online Intermediaries to Create a Website Blocking-Friendly Infrastructure.' (Wilmap, 27 Jan. 2015) <wilmap.law.stanford.edu/news/intermediary-liability-updates-turkey-forcing-online-intermediaries-create-website-blocking> accessed 10 May 2020.

OECD. 'The Economic and Social Role of Internet Intermediaries.' The Economic and Social Role of Internet Intermediaries, OECD, April 2010, <www.oecd.org/internet/ieconomy/44949023.pdf > accessed 25 May 2020.

Offical Gazette of Turkish Republic dated 01.01.2015, <https://www.resmigazete.gov.tr/eskiler/2015/01/20150101-16.pdf?utm_source=ELIG%20Attorneys%20at%20Law&utm_content=ILO%20newsletter%2030985&utm_medium=pdf&utm_campaign=ILO%20Newsletters> accessed 10 May 2020.

'Turkey's general assembly ratifies Internet bill' (Anadolu Agency 26 February 2014) <https://www.aa.com.tr/en/turkey/turkey-s-general-assembly-ratifies-internet-bill/179203> accessed 20 February 2020.

'Turkey's Government Takes New Powers to Censor the Internet' (Economist 24 May 2018) <https://www.economist.com/europe/2018/05/24/turkeys-government-takes-new-powers-to-censor-the-internet> accessed 20 February 2020.

'Turkey: security trumping human rights, free expression under threat' (Council of Europe 14. April 2016) <https://www.coe.int/en/web/commissioner/-/turkey-security-trumping-human-rights-free-expression-under-threat?inheritRedirect=true&redirect=/en/web/commissioner/country-report/turkey> accessed 20 February 2020.

'Turkish Personal Data Protection Law no. 6698' <https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/> accessed 25 May 2020.

Twitter, 'Removal Requests.' <transparency.twitter.com/en/removal-requests.html.> accessed 10 May 2020.

Twitter, 'Transparency Report – Removal Requests, Turkey' (February 2020) <https://transparency.twitter.com/en/removal-requests.html> accessed 10 February 2020.

Case law

Ahmet Yıldırım v. Turkey no 3111/10 ECHR [2012].

App. n. 2013/5653 Supreme Court (Published in the Official Gazette No. 29811 and dated 24 August 2016)

App. n. 2015/18581 Constitutional Court of the Republic of Turkey [2019].

App. n. 2016/165 Constitutional Court of the Republic of Turkey [2017].

Bekir Coşkun [2014] Constitutional Court of the Republic of Turkey 12151 [2015].

Birgün İletişim ve Yayıncılık Ticaret A.Ş. [2015] Constitutional Court of the Republic of Turkey 18936 [2019]

Bogomolova v. Russia no. 13812/09 ECHR [2017]

Cengiz and Others v. Turkey no 48226/10 and 14027/11 ECHR [2015].

Decision n. 2017/5325 Penal Department no. 19 of the Supreme Court [2017].

Emin Aydın [2013] Constitutional Court of the Republic of Turkey 2602 [2014].

Kahn v. Germany no 16313/10 ECHR [2016]

Medya Gündem Dijital Yayıncılık Ticaret A.Ş. [2013] Constitutional Court of the Republic of Turkey 2623 [2015].

Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung eines wirtschaftlich gesunden land- und forstwirtschaftlichen Grundbesitzes v. Austria no. 39534/07 ECHR [2013]

Peck v. the United Kingdom no 44647/98 ECHR [2003]

Reklos and Davourlis v. Greece no. 1234/05 ECHR [2009]

Société de Conception de Presse et d'Edition v. France no. 4683/1 ECHR [2016]

Yaman Akdeniz and Others[2014] Constitutional Court of the Republic of Turkey 3986 [2014].

Turkish titles

Legislation

4721 sayılı Türk Medeni Kanunu 2001.

4982 sayılı Bilgi Edinme Hakkı Kanunu 2003.

5237 sayılı Türk Ceza Kanunu 2004.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlara Müdahale Edilmesi Hakkında Kanun 2007.

5809 sayılı Elektronik Haberleşme Kanunu 2008.

5846 sayılı Fikir ve Sanat Eserleri Kanunu 1951.

6098 sayılı Türk Borçlar Kanunu 2011.

6102 sayılı Türk Ticaret Kanunu 2011.

6698 sayılı Kişisel Verilerin Korunması Kanunu 2016.

Books

Cemil Kaya, İdare Hukukunda Bilgi Edinme Hakkı, Seçkin Yayınları, 2005, s. 29.

M Kemal Oğuzman, Ömer Seliçi ve Saibe Oktay Özdemir, *Kişiler Hukuku* (8th edn, Filiz Kitabevi 2005) 135 [Turkish].

Ş Cankat Taşkın, *İnternete Erişim Yasakları* (1. Baskı, Seçkin 2016).

Ulaş Karan, İfade Özgürlüğü: Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi – 2.

Periodicals

AKKURT, S. S., 'Unutulma Hakkı'nın Kişilik Hakkı Kapsamındaki Kişisel Değerlerle İlişkisi, KTO Karatay Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 3, Sayı: 1, Ocak 2018, Sayfa: 81-10 (Turkish)

ÖNOK, Murat, Kişisel Verilerin Korunması Bağlamında 'Unutulma Hakkı' ve Türkiye Açısından Değerlendirmeler, İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 16, Sayı: 1, Ocak 2017, Sayfa: 155-188 (Turkish)

Digital resources

Güven Köse, Internet'te Sansür Üzerine Bir Değerlendirme, Hacettepe Üniversitesi <https://www.academia.edu/1614699/Internette_Sans%C3%BCr_%C3%9Czerine_Bir_De%C4%9Ferlendirme?auto=download> accessed 10 May 2020.

Case law

Akdeniz v. Turkey, no. 20877/10, 11.03.2014.

AYM, Adalet Mehtap Buluryer Kararı, B. No: 2013/5447, 16.10.2014.

AYM, Ali Rıza Üçer Başvurusu, B. No: 2013/8598, 02.07.2015, 56.

AYM, E. 2012/2015 K. 2014/331.

AYM, Medya Gündem Dijital Yayıncılık Ticaret A. Ş. Başvurusu, B. No: 2013/2623, 11.11.2015.

AYM, N.B.B. Başvurusu, B. No: 2013/5653, 03.03.2016.

AYM, Orhan Pala Başvurusu, B. No: 2014/2983 15.02.2017.

AYM, Sevim Akat Eşki Kararı, B. No: 2013/2187, 19/12/2013.

Yargıtay 9. Hukuk Dairesi, E. 2014/11621 K. 2014/28293, 25.09.2014.

Yargıtay 12. Ceza Dairesi, E. 2015/4349 K. 2016/5349, 30.03.2016.

Yargıtay Hukuk Genel Kurulu, 17.6.2015 T. 2014/4-56 E.-2015/1679.

ELSA Ukraine

Contributors

National Coordinator

Yulia Zhyvchuk

National Academic Coordinator

Ivan Chopyk

National Researchers

Anna-Mariya Luhova

Iryna Stehura

Karina Lytvyniuk

Kateryna Solodovnyk

Sergiy Balabai

Vladislav Zhemerov

Yaroslav Korniienko

Mykyta Kliapets

National Technical Editor

Mykyta Kliapets

National Academic Supervisor

Olga Belyakova

Acknowledgements

We would like to express our sincere gratitude to academic supervisor - Olga Belyakova for her continuous support in drafting this report and related research, her patience, motivation and immense knowledge.

Introduction

The Internet has become a solid platform for promoting human rights and freedoms where the Freedom of Expression plays an important role. The Internet has created new opportunities for information exchange. At the same time, such access inevitably involves serious risks and threats, such as threats of violence and hate speech, coordinated misinformation campaigns, the use of trolls and bots, etc. Ukraine's attempts to counter these threats often pose even more serious risks to Freedom of Expression online and often may be regarded as disproportionate ones. Even though the state has a positive obligation to prevent illegal behaviour online, it may not exercise its power to interfere in the private activity. The state is therefore responsible to create transparent rules for online playground where the participants have a clear understanding of their liability. At the same time, it is necessary to follow the balance in the application of various measures so as not to create a chilling effect of the Freedom of Expression and allow for free dissemination of information.

In our report we focus on the Ukrainian legislation on the freedom of speech, censorship, blocking and filtering of internet content and several more questions. This report is not intended to be interpreted and is not an exhaustive study of the related issues at hand. At the same time, it generally describes the situation with legal regulation of various aspects, thoughts of experts and our personal reflections regarding particular problems. Of course, we tried to access a sufficient number of sources in order to provide an independent and focused overview of the issues. We hope that this report will provide you with needed knowledge of various topics of related Ukrainian legislation on the Freedom of Expression online.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

1.1. Legislation Overview and Limitations

To begin with, the legislation in force to a vast extend regulates traditional media while missing out its online aspect. Yet generally, this does not limit the existing provisions' scope of application. Therefore, the research will reference laws that may not contain provisions regarding online environment *per se*, yet are quite necessary to cover the overall approach.

While the legislation may differ depending on the medium, some provisions are quite similar if not the same. For example, general limitations, or independency, content freedom and state non-interference principles are reflected quite uniformly with minor differences.

The foundation of the Freedom of Expression protection is set by the Constitution of Ukraine which guarantees the right to freedom of thought and speech, and the free expression of the views and beliefs.[2084] Freedom of expression finds its reflection in numerous laws depending on the sector, or medium in question.

General constitutional limitations under which the freedom of speech may be restricted, therefore, include (i) the interests of national security, territorial integrity or public order with the purpose of preventing [public] unrests or crimes, (ii) safeguarding public health, (iii) protection of the reputation or rights of other individuals, (iv) prevention of the confidential information disclosure, or (v) upholding the authority and impartiality of justice.[2085] Such provision is directly mirrored in several laws with some distinct differences that will be stressed hereinafter as well.

The analysis of the Freedom of Expression will further focus, in particular, on censorship and the right to information.

1.2. Censorship

Prohibition of censorship is widely mentioned across the Ukrainian legislation covering various aspects. Constitution of Ukraine formulates the general

[2084] Constitution of Ukraine 1996 <https://zakon.rada.gov.ua/laws/show/254к/96-вр/ed20200101> accessed 29 March 2020, art 34, §1 (Constitution of Ukraine).
[2085] ibid, art 34, §3.

prohibition rule[2086] that is reflected in the laws on broadcasting organisations[2087] and news agencies.[2088] Civil Code also covers the process of creativity and its results.[2089]

The Law 'On Information' describes censorship as any requirement directed, in particular, to a journalist, mass medium, its founder (co-founder), publisher, manager, distributor to coordinate information before its dissemination, or prohibition of or obstruction to any other form of circulation or dissemination of information. It further extends its application to the prohibition of interference with the professional activities of journalists, control over the content of information to be disseminated, suppression of publicly necessary information, prohibition of covering certain topics, displaying certain individuals or disseminating information about them, prohibition of criticising authorities.[2090]

Furthermore, the Law 'On Printed Mass Media (Press)' stipulates that creating and financing state authorities, institutions, organisations, or positions directed at censorship of mass media is forbidden. It goes on to not allow for requirements for prior approval of information disseminated by printed mass media as well as the prohibition of information coming from officials.[2091]

Therefore, it can be concluded that censorship in Ukraine is quite broadly regulated. Although legislation does not directly address censorship online, it is safe to assume that it still falls within the scope of regulation in force due to. At the same time, experts still stress on the lack of proper legislative grounds for

[2086] ibid, art 15, § 3.

[2087] The Law of Ukraine 'On Television and Radio Broadcasting' 1993 №3759-XII <https://zakon.rada.gov.ua/laws/show/3759-12> accessed 21 March 2020, art 5 (Law 'On Television and Radio Broadcasting').

[2088] The Law of Ukraine 'On News Agencies' 1995 №74/95-ВР <https://zakon.rada.gov.ua/laws/show/74/95-вр>accessed 21 March 2020, art 2 (Law 'On News Agencies').

[2089] The Civil Code of Ukraine 2003 №435-IV <https://zakon.rada.gov.ua/laws/show/435-15> accessed 21 March 2020, art 309, § 2(2) (Civil Code of Ukraine).

[2090] The Law of Ukraine 'On Information' 1992 №2657-XII <https://zakon.rada.gov.ua/laws/show/2657-12> accessed 21 March 2020, art 24, §1, 2 (Law 'On Information').

[2091] The Law of Ukraine 'On Printed Mass Media (Press)' 1993 №2782-XII <https://zakon.rada.gov.ua/laws/show/2782-12> accessed 21 March 2020, art 2, §2, 3 (Law 'On Printed Mass Media (Press)').

ensuring the independence of mass media[2092] and usage of indirect censorship by the state authorities despite the prohibition.[2093]

1.3. Right to Information

The Constitution of Ukraine fixes the Right to Information by allowing to freely collect, store, use and disseminate information disregarding the medium.[2094] The Law 'On Information' details this right to include receiving and protection of information. The Law also establishes another ground for limitation in addition to the aforementioned in 1.1 by restricting the exercise when a breach of rights, freedoms, interests of individuals and legal entities may occur.[2095] Moreover, a court may prohibit disseminating information that breaches a right of an individual until such is rectified, if possible.[2096]

Generally, the Law refers to three types of information, access to which can be restricted, that is confidential information, classified information, and information related to a public office.

Confidential information. Here, the Law differentiates between (i) personal data and (ii) other information, access to which is restricted by an individual or legal entity.[2097]

(i) Personal data is therefore defined as any (set of) information related to an individual who is identified or can be specifically identified.[2098] The Law 'On Personal Data Protection' mimics this provision[2099] and sets out related regulatory framework. It is important to emphasise the limits of personal data access restrictions. Experts highlight that 'only the persons of private law can decide which information about them can be treated as confidential, and which - as public'.[2100] Similar idea was also highlighted by the Constitutional Court of

---

2092 Tetiana Prystupenko, 'The State of Legislative Regulation of Domestic Media in the Conditions of New History of Ukraine' (Scientific Notes of the Institute of Journalism, Volume 2 (67), 2017) 30 <http://nbuv.gov.ua/UJRN/Nzizh_2017_2_6> accessed 21 March 2020.

2093 Oksana Soldatenko, 'Information Space on the Internet: Legal Regulation and Control' (Entrepreneurship, Economy and Law, 2018) 138 <http://pgp-journal.kiev.ua/archive/2018/5/27.pdf> accessed 6 May 2020.

2094 Constitution of Ukraine, art 34, §2.

2095 Law 'On Information', art 5, §1, 2.

2096 Civil Code of Ukraine, art 278.

2097 Law 'On Information', art 21, §2.

2098 ibid, Article 11, §1.

2099 The Law of Ukraine 'On Personal Data Protection' 2010 №2297-VI <https://zakon.rada.gov.ua/laws/show/2297-17> accessed 22 March 2020, art 2, §10 (Law 'On Personal Data Protection').

2100 Khrystyna Burtnyk, 'Confidential Information, Information about a Person and Personal Data: Correlation And Regulation', <https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/> accessed 23 March 2020.

Ukraine.[2101] Nonetheless, law can specifically instruct which information shall be treated as confidential. For example, this refers to the information regarding nationality, education, marital status, religious beliefs, health status, date and place of birth,[2102] economic status,[2103] primal data and administrative data about respondents in the course of statistical analysis,[2104] place of residence and stay, person's personal relations with others, including family members, and the other aspects of [private] life.[2105] Such treatment is deemed to be directed at pre-emptive protection of certain information about an individual as otherwise substantial damage may be caused.[2106]

Simultaneously, law can also limit the scope of personal data protection. Such may concern information about persons who were authorised to manage public funds and/or property,[2107] information in the declaration of an individual performing public functions,[2108] information concerning the official authority of an individual related to public functions.[2109] Thus, not all information pertaining to an individual that is personal data can be treated as confidential information and enjoy the same level of statutory protection.

(ii) Furthermore, there is also confidential information that does not fall within the scope of personal data. As mentioned before, the Law refers to such as 'the other information, access to which is restricted by an individual or legal entity'. The regulation of such information is rather scarce. Generally, it can be understood as information, access to which a person has chosen to restrict. When a public authority possesses such information, it may only be disseminated under a specific consent.[2110] Also, specific contractual application of such may be inferred.[2111]

2101 Resolution of the Constitutional Court of Ukraine 2012 № 2-рп/2012 <https://zakon.rada.gov.ua/laws/show/v002p710-12> accessed 24 March 2020 3(2) (Constitutional Court of Ukraine).

2102 Law 'On Information', art 11, §2.

2103 Resolution of the Constitutional Court of Ukraine 1997 № 5-зп <https://zakon.rada.gov.ua/laws/show/v005p710-97> accessed 24 March 2020.

2104 The Law of Ukraine 'On State Statistics' 1992 №2614-XII <https://zakon.rada.gov.ua/laws/show/2614-12> accessed 23 March 2020, art 21, §1.

2105 Resolution of the Constitutional Court of Ukraine 2012.

2106 Dmytro Kotliar, 'Scientific and Practical Commentary to the Law of Ukraine 'On Access to Public Information' (Public Media Center, 2012) 122 <http://access-info.org.ua/wp-content/uploads/2015/12/205.pdf> accessed 23 March 2020.

2107 The Law of Ukraine 'On Access to Public Information' 2011 №2939-VI <https://zakon.rada.gov.ua/laws/show/2939-17>accessed 23 March 2020, art 5, §5 (Law 'On Access to Public Information').

2108 Law 'On Personal Data Protection' art 5, §3(1).

2109 Resolution of the Constitutional Court of Ukraine 2012.

2110 Law 'On Access to Public Information', art 7, §1.

2111 Civil Code of Ukraine, art 862, 895, 1121.

The Law 'On Access to Public Information' brings about some additional regulation. Under the Law, public information is fully accessible unless restricted, and refers to any information owned, received or created by a public authority.[2112] The information may be accessed via official sources such as printed media, websites, etc., or through a specific request.[2113] The Law also prescribes a different threshold for access restrictions. In addition to the protection of interests as aforementioned in 1.1, the Law defines substantial harm to such interests as a required element in case the information is disseminated. Also, such harm shall outweigh the public interest in disclosing the information.[2114] The Law further specifies that the access to information regarding public funds or property management, conditions under which such were received, cannot be limited. It is interesting to notice some more restriction grounds, such as state defence and crime prosecution.[2115]

Classified information. Such is referred to as any information that may harm an individual, society or the state, and may be referred to state, professional, banking, pre-trial investigation or any other related information with a certain level of secrecy.[2116] Specific laws may set the framework for such categories, such as state,[2117] or banking classified information.[2118]

Information related to a public office. Such is referred to any state or local authority office related information connected to (i) strategic office activity, exercising controlling or supervisory functions, decision-making process that precede the public consultation and/or decision-making, or (ii) collected investigative, counterintelligence, or country defence information that is not classified as a state secret. Handling of such information is detailed in the by-laws.[2119]

2112 Law 'On Access to Public Information', art 1.
2113 ibid, art 5.
2114 ibid, art 6, §2.
2115 ibid, art 6, §5.
2116 ibid, art 8.
2117 The Law of Ukraine 'On State Classified Information' 1994 №3855-XII <https://zakon.rada.gov.ua/laws/show/3855-12> accessed 28 March 2020.
2118 The Law of Ukraine 'On Banks and Banking Activity' 2000 №2121-III <https://zakon.rada.gov.ua/laws/show/2121-14> accessed 28 March 2020.
2119 Model instruction on the procedure for keeping records, storing, using and destroying documents as well as other tangible information storage media containing official information as approved by the Cabinet's of Ministers Resolution 2016 №736 <https://zakon.rada.gov.ua/laws/show/736-2016-п> accessed 28 March 2020.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

2.1. Legislation Overview

Overall, there is no specific legislation directly aimed at blocking or takedown of internet content. Provisions may be characterised as mostly scattered and situational allowing for indirect applicability.

The legislation with related provisions to blocking or takedown encompasses:

1. The Law of Ukraine 'On Sanctions' which was applied to enforce blocking on the grounds of national security. For details see 0.
2. Martial and emergency situations laws provide for restrictions applicable to the freedom of speech as allowed for under the Constitution of Ukraine. Such may be used in the context of content blocking. For details see 0.
3. The Civil Code foresees filtering provision in the context of individual rights protection. For details see 0.
4. Criminal Code introduces provisions regarding pornographic material. For details see 0.
5. The Law of Ukraine 'On TV and Radio Broadcasting' and 'On Cinematography' provides specific content filtering. For details see 0 and 0 (in reference to grounds for blocking) and 0 (in reference to hate speech).
6. The Law of Ukraine 'On Telecommunications' establishes a general rule for telecom operators and providers related to child pornography only. For details see 0.
7. The Law of Ukraine 'On Copyright and Related Rights' fixes takedown procedure. For details see 0 (in reference to grounds) and 6 (in reference to intermediate responsibility).

Such laws provide for sporadic coverage of the content takedown/blocking. The legislation was highlighted to remain poor.[2120]

[2120] Maksym Dvorovyi, 'How the Internet will be Regulated in Ukraine in 2017-2019. Risk Assessment and Recommendations' <https://cedem.org.ua/analytics/ukraine-internet-regulation/> accessed 07 May 2020.

2.2. Policy papers

Generally, policy papers simply set the framework and lay out prospects of state policy. These are not exactly legally binding and seldom set goals against which they can be measured to estimate effectives and state of their implementation.

To begin with, the Doctrine on Informational Security determines state interests, potential threats and priorities of state policy in the informational sphere in general while specifically taking a critical focus against the destructive information influence of the Russian Federation in the conditions of the hybrid war. One of such priorities is to adopt legislation that would allow to create a mechanism of detection, fixation, blocking and removal from the information space of the state, in particular from the Ukrainian segment of the Internet, any such information that threatens life, health of Ukrainian citizens, promotes war, national and religious enmity, violent changes of the constitutional order, violation of the territorial integrity of Ukraine, threatens state sovereignty, promotes communist and/or national-socialist (Nazi) totalitarian regimes and their symbolism.[2121] The Doctrine was criticised for being vague in definitions resulting in the uncertainty of implementation mechanisms, disproportionate treatment of the communications providers, the absence of the claimed state and civil society institutions' interoperation mechanisms.[2122] Whereas the Doctrine seems to be quite imbalanced, it is also a framework document with little to no real outcome. It is worth noting that the suggested legislation has not been developed as of the time of this Report.

Furthermore, the same protectionist narrative seems to be reflected in the Cybersecurity Strategy as well as it heavily focuses on a public sector. Even though the wording also suggests a broader applicability, the focus of counteracting potential informational threats from the Russian Federation is still maintained. The Strategy, *inter alia,* mentions the blocking of a certain (identified) information resource or service by telecom operators and providers under a court ruling.[2123]

[2121] Decree of the President of Ukraine 'On the decision of the National Security and Defence Council 'On the Doctrine of Information Security of Ukraine' as of 29 December 2016 №47/2017 <https://zakon.rada.gov.ua/laws/show/47/2017/> accessed 14 April 2020.

[2122] 'Letter №36/1-5 as of 07 March 2017 on the implementation of the Decree of the President of Ukraine as of 25 February 2017 № 47/2017' (2017) <https://inau.ua/document/lyst-no361-5-vid-07032017-shchodo-realizaciyi-ukazu-prezydenta-ukrayiny-vid-25022017-no> accessed 23 February 2020.

[2123] Cybersecurity Strategy of Ukraine as enacted by the Decree of the President of Ukraine as of 15 march 2016 №96/2016<https://zakon.rada.gov.ua/laws/show/96/2016> accessed 14 April 2020.

2.3. Proposals

Amongst a variety of draft laws in recent years, the Draft Law 'On Media'[2124] (the 'Primary Draft Law') deserves attention. It is the first attempt to encompass various regulations concerning different media while updating it to match modern trends.

Thereby, content blocking is introduced as a mean of media liability for the breach of a law on licensing requirements. Blocking is suggested to be enforced irrespective of whether the subject responsible for the breach has been identified. The National Council of TV and Radio Broadcasting would therefore file an administrative lawsuit to be heard in summary proceeding. Whereas website blocking is involved, such restriction may be further enforced by prohibiting internet or hosting service providers, or domain name registrar to suspend providing respective services.[2125] The legitimacy of applying such measures to the internet providers was widely discussed. As a result, it was recommended to exclude internet providers from the list of subjects that can enforce blocking because of technical restrictions. It was stressed that only a website owner, hosting service provider, or domain name registrar may enforce such measures. Also, an additional reference to a court ruling as a ground for applying such measure was recommended to be added. This was made to redline the edge of intermediaries' responsibility for internet content as under the general rule telecom providers are not responsible for the content of information transmitted by their networks.[2126]

In the context of online media, the applicability of content blocking is rather vague. The Primary Draft Law differentiates three degrees of violation depending on their harshness.[2127] However, no clear diction between a measure of restriction and a degree of violation is made. Thus, it may be assumed that minor violation can also entail blocking, which may be seen as a ground for potential abuse.

Furthermore, the Primary Draft Law establishes specific content restrictions, such as those referring to general freedom of speech protection limitations (see 1.1 for the details), hate speech, pornographic material, propaganda of terrorism, violence against animals, drugs abuse, information that denies or justifies the

---

2124 The Draft Law 'On Media' №2693 as of 27 February 2019 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812> (Draft Law 'On Media').

2125 Draft Law 'On Media', art 97, §3(3), §6, §7.

2126 'Representatives of Provider Associations Discussed the Draft Law of Ukraine 'On Media' with the Committee of Humanitarian and Information Policy' (23 January 2020) <http://www.appk.org.ua/ru/news/show/predstavniki-asots%D1%96ats%D1%96i-provaider%D1%96v-obgovorili-z/page/4/> accessed 20 April 2020.

2127 Draft Law 'On Media', art 112.

criminal nature of the communist totalitarian regime of 1917-1991 in Ukraine, the criminal nature of the national-socialist (Nazi) totalitarian regime, etc.[2128] Further content limitations may be applied with regards to the protection of minors. It should be noted though that the Primary Draft Law does not provide for means of access restriction to information online that constrains content limited to minors. Effectively, this may mean that such content limitations may be applicable to any content irrespective of the viewer advisory online.

In respect of the content blocking, the Primary Draft Law has received generally positive recommendations. In particular, it was stressed that 'the [blocking] mechanism complies with the requirements for restrictions that may be imposed on the online media outlined in the Manila principles and the case law of the EU Court of Justice. In particular, access to websites will be restricted only by court order, and the restrictions themselves will depend on the nature of the content'.[2129] On the contrary, experts criticise the blocking measures to be 'excessive and disproportionate'. The particular reference is made to the generality of the ban, unclear duration of application, and too broad wording for the grounds for blocking. Potential threats of chilling effects on the Ukrainian media and state enforced censorship are stressed.[2130]

Alternatively, a Draft Law 'On Media in Ukraine'[2131] (the 'Alternative Draft Law') was proposed. In general, the Alternative Draft Law largely repeats the main provisions of the Primary Draft Law. However, certain differences need to be highlighted.[2132] In particular, the Alternative Draft Law provides for a clearer procedure for making the decision of the National Council of TV and Radio Broadcasting to turn to the court for a blocking ruling. It is worth noting that such a decision is suggested to be made in strict accordance with Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights.[2133] The Chief Scientific and Expert Department considered that the Draft Law №2693-

---

2128 ibid, art 37.

2129 'About the media law and the internet, or Regulate Unregulated' (28 January 2020) <https://detector.media/rinok/article/174258/2020-01-28-pro-mediinii-zakon-ta-internet-abo-vregulyuvati-nevregulovane/> accessed 20 April 2020.

2130 Dr. Joan Barata Mir, Commissioned by the OSCE Representative on Freedom of the Media, 'Legal Analysis of the Draft Law Of Ukraine 'On Media' (February 2020) 29 <https://www.osce.org/representative-on-freedom-of-media/447508?download=true&fbclid=IwAR1n5cWdx8zGWTktJ4k-WmPEgNt9-azjZWsUICwJC0i-knMn840XCqmCTpI> accessed 11 May 2020.

2131 The Draft Law 'On Media in Ukraine' №2693-1 as of 15 January 2020 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67886> (Draft Law 'On Media in Ukraine').

2132 'The Draft Law 'On media' is being examined by the Council of Europe' (21 January 2020) <http://www.golos.com.ua/article/326485> accessed 30 April 2020.

2133 Draft Law 'On Media in Ukraine', art 106.

1 has the positive developments related to the attempt to systematise current rules on the regulation of media services, but at the same time, it still contains a number of conceptual shortcomings that make its adopting vulnerable.[2134] That is why the Committee of Humanitarian and Information Policy has decided to recommend to the Ukrainian Parliament to adopt the Primary Draft Law. Nevertheless, the possibility of 'integrating the best parts of the alternative Draft Law №2693-1 with the Draft Law №2693 into a single act' is still under consideration.[2135]

Another proposal to adopt specific blocking instruments is set in the Draft Law aimed at gambling regulation (the 'Draft Law 'On Gambling'). The idea is to impose an obligation on the hosting and telecom providers to restrict access to online services operating without a licence upon a request of a to-be-created state authority.[2136] However, this proposal was criticised to breach, among others, the open accessibility and liability limitation principles which contradict the current regulation. Experts also highlighted that the access cannot be blocked by the telecom operators and providers due to technical constraints. Instead, this obligation was suggested to be imposed on website owners, domain name registrants and hosting services providers.[2137]

There were also attempts to increase extrajudicial measures for blocking. Under the Draft Law №6754 the State Service of Ukraine on Food Safety and Consumer Protection was suggested to be granted the authority to suspend access to websites when a seller fails to provide access to the information about a product on its website.[2138] Experts stressed that it was an attempt to increase administrative pressure on Ukrainian business and does not help to protect the

[2134] Conclusion on the Draft Law 'On Media in Ukraine' (17 January 2020) <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67886> accessed 30 April 2020.

[2135] Committee of Freedom of speech supports the Draft Law 'On Media' (06 February 2020) <https://yurincom.com/legal_news/komitet-z-pytan-svobody-slova-pidtrymav-proekt-zakonu-pro-media/> accessed 30 April 2020.

[2136] Draft Law 'On the State Regulation of Activities Related to Organizing and Conducting Gambling' as of 18 December 2019 №2285-A <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67682> accessed 10 May 2020, art 25, §2, 3, Ch. XII art 10, §5 (Draft Law 'On Gambling').

[2137] Letter [by the Internet Association of Ukraine] № 05/1-5 as of 23 January 2020 to the Supreme Council on providing comments to the Draft Law 'On State Regulation of Activities Related to Organizing and Conducting Gambling' (№ 2285-A as of 18 December 2019) <https://inau.ua/document/lyst-no-051-5-vid-23012020-vru-shchodo-nadannya-zauvazhen-do-zakonoproektu-pro-derzhavne> accessed 10 May 2020.

[2138] The Draft Law 'On amendments to the Law of Ukraine 'On Consumer Protection' and some legislative acts of Ukraine on measures to de-shadow the activities of e-commerce entities' №6754 as of 17 July 2017 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62329> accessed 12 May 2020, Ch 1art 3.

rights of consumers from poor quality of the e-commerce services.[2139] Draft Law №6754 was revoked in 2019. The Draft Law №6688 proposed the possibility of temporary blocking under the decision of a prosecutor, investigator or the National Security and Defence Council of Ukraine.[2140] The Draft Law №6688 was recognised to have a rather negative influence on digital rights,[2141] and was even characterised as the anti-democratic and dictatorial one.[2142] Draft Law №6688 was also revoked in 2019.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

3.1. National Security and Integrity

As an indirect continuation of the protectionist policy against potential informational threats from the Russian Federation as envisaged by particular policy papers (refer to 0), Ukrainian authorities enforced blocking to restrict access to several Russian websites in order to fight hybrid war and propaganda.[2143]

The instrument was enforced through the Law of Ukraine 'On Sanctions' allowing the National Security and Defence Council of Ukraine (NSDC), a presidential coordination body in the area, to impose particular restrictions. The Law does not explicitly provide for blocking as one of the permissible instruments. Although, it allows for 'other sanctions in accordance with the principles of their application as established by this Law',[2144] which may vaguely be interpreted to allow for *any imaginable* sanctions if they correspond to certain

---

2139 'InAU proposes not to approve Draft Law №6754, which increases administrative pressure on Ukrainian business' (25 July 2017) <https://inau.ua/news/inau-proponuye-ne-pogodzhuvaty-zakonoproekt-6754-yakyy-posylyuye-administratyvnyy-tysk-na> accessed 13 May 2020.

2140 The Draft Law 'On amendments to certain legislative acts of Ukraine about counteraction to threats to national security in the information sphere' №6688 as of 12 July 2017 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236> accessed 12 May 2020, Ch 1, art 5.

2141 Maksym Dvorovyi, 'How the Internet Will Be Regulated in Ukraine in 2017-2019. Risk Assessment and Recommendations' (06 November 2017) <https://cedem.org.ua/analytics/ukraine-internet-regulation/> accessed 12 May 2020.

2142 Coalition 'For Free Internet', Bill №6688 may lead to the complete cessation of some information resources (02 July 2018) <https://detector.media/infospace/article/139000/2018-07-02-zakonoproekt-6688-mozhe-prizvesti-do-povnogo-pripinennya-diyalnosti-deyakikh-informresursiv-koalitsiya-za-vilnii-internet/> accessed 30 April 2020.

2143 Alec Luhn, 'Ukraine blocks popular social networks as part of sanctions on Russia' (16 May 2017) <https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war> accessed 08 May 2020.

2144 The Law of Ukraine 'On Sanctions' 2014 №1644-VII <https://zakon.rada.gov.ua/laws/show/1644-18> accessed 02 April 2020, art 4, §1(25) (The Law 'On Sanctions').

criteria. Interestingly enough, any decision of NSDC needs to be enacted by a presidential decree in order to be enforced.[2145] With that being said, such decisions are applicable only to executive authorities.[2146]

The NSDC can impose sectoral and personal sanctions for the purpose of national interests, national security, sovereignty and territorial integrity of the state protection, counteraction of terrorist activity, as well as prevention of violation, restoration of violated rights, freedoms and legitimate interests of Ukrainian citizens.[2147]

The freedom of speech restriction in the interests of national security, territorial integrity, or public order is one of the derogations allowed under the Constitution of Ukraine (refer to 1.1).[2148] Therefore, the balance between protecting the fundamental freedoms and observing the state's own integrity deserves attention, even more so considering current situation in Ukraine. Experts stress that as the information can be weaponised it creates difficulties in creating proper counter-action mechanisms to deal with Russian disinformation.[2149] The lack of proper internet environment regulation leaves certain decisions to be taken on a case-by-case basis.[2150]

In this aspect it is necessary to consider the notorious Decree of the President of Ukraine №133/2017.[2151] The Decree enacted the Decision of NSDC under which several Russian websites, such as VKontakte and Odnoklassniki social network, Mail.ru email service provider, Kaspersky Lab cybersecurity and anti-virus provider and Dr. Web anti-malware provider, and Yandex search engine company (39 websites in total) were blocked.[2152] Notably, the wording in the

2145 The Law of Ukraine 'On the National Security and Defence Council of Ukraine' 1998 №183/98-ВР <https://zakon.rada.gov.ua/laws/show/183/98-вр> accessed 03 April 2020, art 10, §3.

2146 ibid, art 10, §4.

2147 The Law of Ukraine 'On Sanctions', art 1, §1.

2148 Constitution of Ukraine, art 34, §3.

2149 'Freedom of speech vs. information security? Key quotes from UkraineWorld's event at Kyiv Security Forum 2019' (15 April 2019) <https://netfreedom.org.ua/article/rozvagi-vidigrayut-znachno-bilshu-rol-u-viborchomu-procesi-nizh-racionalni-debati> accessed 24 February 2020.

2150 'DW Akademie, #speakup barometer. Ukraine. Accessing Digital Participation' (2019) <https://www.dw.com/downloads/49486400/speakup-barometer-ukraine-full-report.pdf> accessed 21 February 2020.

2151 Decree of the President of Ukraine as of 15 May 2017 №133/2017 'On the decision of the National Security and Defence Council of Ukraine as of 28 April 2017 'On the application of personal special economic and other restrictive measures (sanctions)' <https://zakon.rada.gov.ua/laws/show/ru/133/2017/> accessed 03 April 2020 (Presidential Decree №133/2017).

2152 Decision of the National Security and Defence Council of Ukraine as of 28 April 2017 <https://zakon.rada.gov.ua/laws/show/ru/n0004525-17/> accessed 03 April 2020.

Decision suggests that Ukrainian *internet* providers were restricted in providing access services to the specified links and webpages.[2153]

In light of such a wording, the Law of Ukraine 'On Telecommunications' neither establishes general blocking obligations for telecom operators, nor provides for any other possibility to enforce the NSDC's decision. The only obligation the Law refers to is blocking access to resources through which child pornography is disseminated under a court ruling.[21542155]Even then, this particular provision does not concern telecom providers, but only telecom operators.[2156] Moreover, the Law does not provide for the definition of '*internet* providers' as mentioned in the Decision.

On top of all that, neither the Presidential Decree, nor the NSDC Decision provides for any mechanism that would allow the blocking to be enforced. While the NSDC's decisions are applicable to the executive authorities, as mentioned above, no mention is made how such is to be enforced by private law telecom operators or providers. The contextual analysis of the said regulation makes it safe to assume that the Decision and the Decree were adopted with an effective *inability* to be implemented. At least, in theory. Practically, the blocking was still enforced.

NSDC's numerous other decisions, under which numerous websites affiliated with the sanctioned persons were blocked, were criticised as breaching the due process and characterised as manifestation of unlimited discretion of the state power.[2157]

As analytical sources highlight the necessity of media pluralism and balanced blocking approach,[2158] the actions of the state regarding freedom of speech restrictions may be interpreted as disproportionate. At the same time, such statement can be regarded as one-sided since it only implies the *possibility* of the

---

2153 The list of legal entities sanctioned under the Decision of the National Security and Defence Council of Ukraine as of 28 April 2017, annexed to the Decision <https://zakon.rada.gov.ua/laws/file/text/54/f467150n25.pdf> accessed 03 April 2020.

2154 The Law of Ukraine 'On Telecommunications' 2003 №1280-IV <https://zakon.rada.gov.ua/laws/show/1280-15> accessed 02 April 2020, art 39, §1(18).

2155 Rules for Providing and Receiving Telecommunication Services as adopted by the Decree of the Cabinet of Ministers 2012 № 295 <https://zakon.rada.gov.ua/laws/show/295-2012-п> accessed 07 June 2020.

2156 ibid, art 39, §2.

2157 'Legal analysis of the presidential decree on blocking sites' (08 June 2018) <https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html> accessed 21 February 2020.

2158 Olga Kyryliuk, 'Freedom of Expression in Times of Conflict: Ukrainian Realities. Analytical report' (2017) <https://cedem.org.ua/wp-content/uploads/2017/08/Freedom-of-Expression_Report_Ukraine_DDP_ENG.pdf> accessed 22 February 2020.

power misuse. It is vital to analyse the exact nature of sanctioned websites and the context of the information published online as some critics state that 'the priority aim of applying sanction is not restricting access to anti-Ukrainian propaganda and disinformation materials but the public recognition of Russia-controlled resources as constituting a threat to the national security, sovereignty, and territorial integrity of Ukraine.'[2159]

3.2. Extraordinary Circumstances

In addition to general limitation in the context of emergency situations, emergency situation law introduces the following blocking/filtering measures applicable only under the circumstances of mass violation of public order:

— ban on the production and distribution of information materials that can destabilise the situation;

— regulation of the civilian television and radio centres' operation, prohibition of the operation of amateur radio transmitters and radio-emitting devices for personal and collective use;

— specific rules for using communications and transmitting information over computer networks.[2160]

In respect of the martial law, the following blocking/filtering measures may be implemented:

— regulate the work of telecom enterprises, printing companies, publishing houses, broadcasting organisations, television and radio centres and other enterprises, institutions, organisations and cultural institutions and the media,

— use local radio stations, television centres and printing houses for military purposes and providing military intelligence and population;

— prohibit the use of personal and collective transceivers and the transmission of information via computer networks.[2161]

Even though none of the aforementioned measures specifically provides for content blocking or filtering, the wording suggests that such may be indeed inferred. It is worth mentioning that there has not been a single case of the

[2159] Dmytro Zolotukhin, 'Ukraine: FAQ on the Freedom of Speech Issues in Terms of Hybrid War' (07 August 2018) <https://medium.com/@postinformation/ukraine-faq-on-the-freedom-of-speech-issues-in-terms-of-hybrid-war-5370e84139b1> accessed 24 February 2020.

[2160] Law 'On the Legal Regime of Emergency State', art 18, §2(6-8).

[2161] Law 'On the Legal regime of Martial State', art 8, §1(18).

emergency law and only one instance of the martial law declaration in Ukraine since 1991.[2162] In the latter case, no known content blocking or filtering measures were applied as a part of restrictive measures specifically under the martial law.

3.3. Civil Law Restrictions

Several provisions govern filtering possibilities. Whereas any individual right of a person is breached though dissemination of information via a specific medium, such information can be prohibited from being disseminated under a court ruling until rectified. If rectification is not possible, a medium, through which the information is disseminated, may be removed from circulation. It is necessary to highlight that the provision has a heavy accent on traditional media, such as newspapers, books, movies, TV- and radiobroadcasting.[2163]Although, this does not preclude it from application in online environment.

Civil Code also provides for a specific self-defence instrument that allows to enforce any means of counteraction which are not prohibited by law and do not contradict the moral principles of society.[2164]

3.4. Criminal Law Restrictions

Evidently, pornographic material is prohibited to the extent of import, sale, dissemination, manufacture, storage, transportation, coercion to participation in its creation. The prohibition may, in particular, concern film and video production, computer programs of pornographic nature.[2165] Such provisions are grounded on the general pornographic content prohibition rules as fixed in the Law of Ukraine 'On the Protection of Public Morale'.[2166] However, there are no provisions covering specifically content blocking, removal or filtering of such content. Moreover, the only reference to the blocking mechanism regarding child pornography content is made in the Law 'On Telecommunications' as mentioned in 3.1 above.

2162 Decree of the President of Ukraine 'On the decision of the National Security and Defence Council of Ukraine as of 26 November 2018 'On emergency measures to ensure state sovereignty and independence of Ukraine and the declaration of martial law in Ukraine' as of 26 November 2018 № 390/2018<https://zakon.rada.gov.ua/laws/show/390/2018> accessed 14 April 2020.

2163 Civil Code of Ukraine, art 278, §2.

2164 ibid, art 19.

2165 The Criminal Code of Ukraine 2001 №2341-III <https://zakon.rada.gov.ua/laws/show/2341-14> accessed 29 April 2020, art 301 (Criminal Code of Ukraine).

2166 The Law of Ukraine 'On the Protection of Public Morale' as of 20 November 2003 №1296-IV <https://zakon.rada.gov.ua/laws/show/1296-15> accessed 29 April 2020, art 2, §1 (Law 'On the Protection of Public Morale').

3.5. Broadcasting

Particular filtering limitations are set in regards to the TV- and radio broadcasting in the light of inadmissibility of abuse of the freedom of broadcasting organisations' activity. Therefore, it is prohibited to use broadcasters to disseminate information that contains:

— calls for a violent change in Ukraine's constitutional order, aggressive war;

— hate speech or propaganda of discrimination;

— unreasonable display of violence;

— pornographic content, propaganda of drugs abuse;

— fortune-telling or commercial services for traditional or alternative medicine;

— promotion or propaganda of the authorities of the aggressor state and their individual actions justifying or recognising the legitimate occupation of the territory of Ukraine;

— violation of rights and interests of individuals and legal entities.[2167]

The Law, however, does not specify the means to filter such content.

Particular blocking and takedown measures concerning hate speech are foreseen under the broadcasting law. For more details refer to 8.3.

3.6. Cinematography

As the national TV-broadcasters upload films on their official websites, content regulation of cinematography should be assessed. In particular, the distribution and demonstration of films that promote war, violence, cruelty, fascism and neo-fascism, are aimed at eliminating the independence of Ukraine, incitement of interethnic, racial, religious hatred, humiliation of the nation, humiliation or contempt of the state language, disrespect for national and religious shrines, humiliation of individuals as well as drug addiction, substance abuse, alcoholism and other bad habits, pornographic is banned.[2168] This lies in conformity with the provisions of Law 'On the Protection of Public Morale'.[2169] Moreover, it is

[2167] Law 'On Television and Radio Broadcasting', art 6.

[2168] The Law of Ukraine 'On Cinematography' 1998 № 9/98-ВР <https://zakon.rada.gov.ua/laws/show/9/98-вр> accessed 30 April 2020, art 15, §3(3) (Law 'On Cinematography').

[2169] Law 'On the Protection of Public Morale', art 2.

prohibited to distribute and demonstrate films which contain, in particular, propaganda of or popularise the aggressor state, or justify or recognise the lawful occupation of the territory of Ukraine.[2170]

3.7. IP Infringement

Also, in case of copyright and related rights infringements, the procedure of take-down notice does exist.

Under the Law of Ukraine 'On Copyright and Related Rights',[2171] an owner of a specific right may request the website owner or hosting provider to terminate the perceived violation of his/her right. The request shall be submitted by an attorney who serves as an intermediary. Should the request satisfy the necessary conditions to approval, the content shall be removed within 48 hours.

3.8. Compliance with ECHR requirements

Any national law that entrenches blocking, take-down or filtering of the online content must justify such kind of interference under Article 10 of the European Convention on Human Rights, namely, meet three conditions:

- provide sufficient legal norms for the relevant measure ('prescribed by law');
- prove that goal pursued is necessary in a democratic society;
- show that legal provisions and the particular measure based on them are proportionate.

Additional countermark applied by the European Court of Human Rights requires laws that prescribe prior or post-expression interference to be public, accessible, predictable and foreseeable to enable a citizen to regulate their conduct.[2172] It can be assumed that these criteria are fulfilled to some extent in the Ukrainian legislation. Mostly, grounds for blocking/filtering are clearly stipulated. At the same time, wording can seem to be flawed. For instance, experts highlight that the derogations allowed under the Constitution of Ukraine (refer to 1.1) do not specify 'necessity in democratic society' criterion which is only balanced out by the possibility of the direct ECHR application.[2173] However,

---

2170 Law 'On Cinematography', art 15[1].

2171 The Law of Ukraine 'On Copyright and Related Rights' 1993 №3792-XII <https://zakon.rada.gov.ua/laws/show/3792-12> accessed 02 May 2020, art 52-1, §1, 7 (Law 'On Copyright and Related Rights').

2172 *The Sunday Times v. the United Kingdom*, no. 6538/74 <http://hudoc.echr.coe.int/eng?i=001-57584> accessed 30 April 2020.

2173 O. Burmagin, L. Opryshko, 'Freedom of Speech on the Internet. A Practical Guide' (NGO 'Human Rights Platform', 2019) 8 <https://www.ppl.org.ua/wp-content/uploads/2019/02/СВОБОДА-СЛОВА-В-ИНТЕРНЕТЕ.pdf> accessed 12 May 2020.

Ukrainian legislation does not always appear to be precise and predictable in the application. For example, while banning the dissemination of pornographic material, the law does not specify legal instruments that can be applied to prevent sharing the content online. The ambiguousness of the Law of Ukraine 'On Sanctions' (refer to 3.1) gives green light to unlimited margin of appreciation when imposing sanctions by the state authority. The absence of enforcing mechanisms under the Decree of the President of Ukraine №133/2017 contributes to the obstacles in the application. Experts also highlight that the provisions of the Decree appear to be disproportionate towards its lawful aim and does not fulfil 'necessary in a democratic society' criterion'.[2174] Draft legislation seems to have similar flaws (refer to 2.3). We can conclude that some national legal acts do not meet the ECHR requirement concerning the quality of law. This makes them ambiguous and leads to the arbitrary usage of their provisions.

3.9. Judicial review

Presidential Decree №133/2017 as mentioned in 2.1 above has also been scrutinised by the court. In the case П/800/217/17, the NGO 'Autonomous Advocacy' filed a lawsuit against the President of Ukraine with a demand to declare illegal and repeal the provisions of the Presidential Decree №133/2017 concerning blocking claiming the restriction of the plaintiff's right to the free usage, dissemination and storage of information. The court stated that the sanctions imposed by the Decree of the President of Ukraine restrict the right of access, in particular, to certain internet resources, which can be considered as interference with the guaranteed under Article 10 of the Convention [European Convention for the Protection of Human Rights and Fundamental Freedoms] freedom to receive and impart information and ideas without interference by public authorities and regardless of frontiers. However, as the court highlights, such interference by the state is not a violation of these freedoms, since the possibility of its introduction is provided, in particular, by the Constitution of Ukraine (part three of Article 34), Law №1644-VII (fifth paragraph of the preamble, part one of Article 1, part three of Article 5) [the Law 'On Sanctions'] and Law №2657-XII (part two of Article 6, part two of Article 7) [the Law 'On Information'] and has a legitimate purpose, specified in the mentioned regulations: the need for immediate and effective response to threats to the national security of Ukraine. The stated purpose is in accordance with Article 10, paragraph 2, of the Convention, according to which restrictions on the

[2174] 'Legal Analysis of the Presidential Decree on Website Blocking' <https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html> accessed 12 May 2020.

freedoms guaranteed by this Article […] may be provided in the interests of national security. The court then proceeds to highlight that under the Decision of the NSDC as of 28 April 2017 the sanctions are aimed, in particular, at restricting the access of internet users to resources or services that threaten the national interests and security of Ukraine. However, the court finds that the restrictions established by Decree of the President of Ukraine №133/2017 of 15 May 2017 are such that they meet the criterion of 'necessity in a democratic society', since there was an urgent need for their introduction and further continuation in view of the recognised facts of aggression against Ukraine.[2175] Thus, the court concluded that the plaintiff's rights and freedoms had not been violated. It was also confirmed that the President of Ukraine acted in due course of maintaining the necessary balance between any adverse effects on the rights, freedoms and interests of the person and the purposes to which this decision (action) is directed, i.e. proportionally.[2176] Thereby, the court upheld its previous decision in relatively same cases.[21772178]

Furthermore, it appears that the lack of blocking/filtering mechanisms results in the ineffectiveness of both civil and criminal procedural law in Ukraine. Thus, court decisions may set new legal vectors and influence the enforcement.

Firstly, controversial information or value judgements cannot be deleted from the Internet. In the case №2/686/2114/18, a claimant pleaded the court to order a television network to remove a story about him/her raising funds among parents at school to buy a gift on the occasion of Ukrainian Armed Forces Day. It was claimed that information from a story was not true, degraded honour, dignity and business reputation of the claimant. Information used by the journalists in this story was obtained from an interview, while no evidence of damage to the claimant's reputation was proved. The court ruled that the claim to remove controversial information is not sufficiently proven in law, and the satisfaction of the claim may be considered to facilitate censorship.[2179]

A similar approach was taken in the case №2/640/1194/17 where a claimant demanded to erase inaccurate information from a story published by an information agency. A court ruled that a critical assessment of certain facts,

---

2175 *Case №П/800/217/17* (05 June 2019) (Grand Chamber of the Supreme Court of Ukraine), §40–43 <http://www.reyestr.court.gov.ua/Review/82738705> accessed 06 April 2020.

2176 ibid, §47.

2177 *Case №800/321/17* (13 June 2018) (Grand Chamber of the Supreme Court of Ukraine) <www.reyestr.court.gov.ua/Review/75286971> accessed 06 April 2020.

2178 *Case №800/205/17* (20 December 2018)(The Supreme Court of Ukraine) <www.reyestr.court.gov.ua/Review/78808026> accessed 06 April 2020.

2179 *Case №2/686/2114/18* (04 December 2018) (Khmelnytskyi City district court) <http://reyestr.court.gov.ua/Review/78885244> accessed 10 February 2020.

shortcomings, opinions, and judgments cannot be used as a reasoning for satisfying claims to the rebuttal of information since it would be a violation of the Constitution of Ukraine, which guarantees the right to freedom of speech by prohibiting censorship. Therefore, whether or not subjective judgements are credible is not subject to be challenged in a court of law.[2180]

Such cases demonstrate that the ban on censorship covers any and all content, information or data regardless of their source of publishing. Since Freedom of Expression entitles anyone to a right to articulate own ideas and beliefs, some of these ideas may be controversial or contain subjective judgements, yet still preserve their protection under the law.

Secondly, the law protects the freedom of political debate on the internet. The approach towards the prohibition of censorship online seems to be prevalent in court cases including the cases regarding politically exposed persons.

For example, in the case №2/0274/820/15 where a claimant (a local deputy) argued the damaged dignity and reputation in an online article. In addition to applying the approach described above, the court also referenced the Declaration on Freedom of Political Debate in the Media, stating that a local deputy is subject to close public scrutiny and may face strong criticism. Thus, the court denied the claim to erase the article, yet did compel the internet medium to amend the article to state that a criminal proceeding against the local deputy was closed. The proceeding was mentioned in the article without such a note which the court found to be a violation of the *bona fides* principle.[2181]

The Declaration on Freedom of Political Debate in the media was also applied in case №296/418/15-c where a director of a local public fiscal authority's branch pleaded to remove an online article speculating that he was involved in malicious prosecution, corruption schemes and bribery. The court once again reminded that according to Article 30 of the Law 'On information', there shall be no liability for expressing personal opinion in a form of a subjective judgement unless they construe defamation (libel or slander). The court also stated that since a fiscal authority director's work is of public interest according to the Council of Europe Parliament Assemble Resolution 1165 (1998), he is a public figure meaning that the Declaration applies to his case, leading for it to be dismissed.[2182]

[2180] *Case №2/640/1194/17*(29 May 2017) (Kyiv district court of Kharkiv) <http://reyestr.court.gov.ua/Review/66893382> accessed 10 February 2020.

[2181] *Case №2/0274/820/15*(11 December 2015)(Berdychiv district court of Zhytomyr region) <http://reyestr.court.gov.ua/Review/54274488> accessed 10 February 2020.

[2182] *Case №296/418/15-c*(29 March 2016) (Zhytomyr region appellate court) <http://reyestr.court.gov.ua/Review/56849990> accessed 10 February 2020.

With regards to website blocking in criminal proceedings, particular court rulings were widely criticised to breach the due process. As such, the access to 19 websites was blocked with regards to measures ensuring criminal proceedings. Experts stressed the breach of due process with regards to identification of material evidence that may be seized and the requirements of applicable law regarding the obligations of telecom service providers.[2183]

As of now, no landmark court rulings in Ukraine regarding blocking/filtering were issued by the Supreme Court, the position of which would have been obligatory to take into consideration by the lower courts. However, this can actually be seen as a positive sign for the state of freedom of speech on the Internet in Ukraine.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

Due to the increasing governmental pressure to introduce blocking/filtering measures in the recent years, civil society tends to create a tension opposing to the imbalanced proposals.[2184] Some examples related to contributing to the state policy or answering particular proposals and actions from the state are described throughout the research. This part will be devoted to instances not mentioned anywhere else.

Some projects were initiated to target specific content filtering. For example,[2185] Skarga.ua was initiated in 2009 as a result of a memorandum between the National Commission on Public Morale and the Internet Association of Ukraine.[2186] The project allows to contribute to tackling illegal online content (juvenile pornography, racial or national intolerance, terrorism or overthrow of constitutional order agitation) by submitting a complaint.[2187] Since then the

2183 Vita Volodovska, Maksym Drovovyi, 'Human Rights Online: Agenda for Ukraine' (2019) 15 <https://dslua.org/wp-content/uploads/2019/12/DRA_FINAL_English.pdf> accessed 10 February 2020 (Human Rights Online: Agenda for Ukraine).

2184 Freedom of the Net Report, 2018 <https://freedomhouse.org/country/ukraine/freedom-net/2018> accessed 10 May 2020.

2185 Skarga, Official website of the Project <http://www.skarga.org.ua/> accessed 10 May 2020.

2186 'Internet Association of Ukraine signs memorandum of cooperation with NEC on Protection of Public Morale' (20 March 2009) <http://khpg.org/index.php?id=1237560807> accessed 10 May 2020.

2187 'InAU launches Skarga.ua project to eradicate violence on the Internet' (22 June 2009) <https://press.unian.ua/press/975381-inau-rozpochinae-proekt-skargaua-iz-vikorinennya-nasilstva-v-interneti.html> accessed 10 May 2020.

National Commission was liquidated,[2188] and the Project seems to produce no particular results.[2189]

Particular efforts are aimed at consolidating private sector associations to filter specific illegal content resulting in several framework documents. For example, the Memorandum of the Information Initiative on Protection of Freedom of Speech aims at protecting journalistic activity on the Internet, the independence of internet media journalists from groups of influence on the market, the creation of a positive image of the Internet as an information resource and respect for user's rights,[2190] the Memorandum on the Protection of Minors in the Provision of Broadcasting Services - at filtering content, harmful to minors, and setting restrictions for broadcasting of such content.[2191]

Internet providers may also stop providing their services to clients. For example, Ukrtelecom, one of the internet service providers, may stop providing services for the use of its network for immoral actions, violation of civil order, honour and dignity of citizens, which may lead to a decrease in the quality of services.[2192] Another internet provider, Kyivstar, may refuse to send information or remove it from servers if it violates Ukrainian law.[2193]

2188 Decree of the Cabinet of Ministers of Ukraine 'On the Liquidation of the National Expert Commission for the Protection of Public Morale' as of 27 May 2015 №333 <https://zakon.rada.gov.ua/laws/show/333-2015-п> accessed 10 May 2020.

2189 'The Internet Association of Ukraine presented the key priorities of its security strategy in the field of information technology' (11 February 2020) <https://press.unian.ua/press/10869098-internet-asociaciya-ukrajini-predstavila-klyuchovi-prioriteti-svoyeji-strategiji-borotbi-za-bezpeku-u-sferi-informaciynih-tehnologiy-video.html> accessed 10 May 2020.

2190 Memorandum of the Information Initiative on Protection of Freedom of Speech (19 June 2011) <https://inau.ua/komitety/komitet-inau-z-pytan-zahystu-prav-lyudyny-ta-svobody-slova/memorandum-informaciynoyi> accessed 04 February 2020.

2191 'Provider Associations have published a Memorandum on the protection of minors in the provision of software services' (28 April 2015) <https://detector.media/rinok/article/106536/2015-04-28-asotsiatsii-provaideriv-oprilyudnili-memorandum-shchodo-zakhistu-nepovnolitnikh-pid-chas-nadannya-programnikh-poslug/> accessed 10 May 2020.

2192 Terms and procedure for providing telecommunication services by Ukrtelecom <https://ukrtelecom.ua/upload/iblock/cfa/326d383d23eb968f7d7d4adb98735867.pdf> accessed 10 May 2020.

2193 Terms of telecommunications services by Kyivstar <https://ukrtelecom.ua/upload/iblock/cfa/326d383d23eb968f7d7d4adb98735867.pdf> accessed 10 May 2020.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

5.1. Legislation Overview

Although seeing these terms being used as synonyms is quite common, a general clarification is needed for better understanding. From a methodological standpoint, the Right to be Forgotten (or, the Right to Erasure), as widely used in Europe, is generally associated with the right to request personal data to be deleted with limitations of a more general nature. Whereas the right to delete, as fixed in some of the US legal acts, can be generally characterised as a narrower manifestation of the right to privacy in a specific industry or sphere, limiting scope of persons exercising this right to consumers only.[2194]

The Right to be Forgotten has greatly evolved since the Data Protection Directive 1995[2195] and by now has a wider scope of application as fixed in the General Data Protection Regulation 2016 (the 'GDPR').[2196] For instance, the extended scope also includes the erasure from search engines[2197] following Google Spain v AEPD and Mario Costeja González judgement.[2198] However, neither rulings of the European Court of Justice, nor the GDPR are sources of law in Ukraine, although the latter may apply if targeting criterion of Article 3(2) applies.

It may be thus inferred that since the Law of Ukraine 'On Personal Data Protection'[2199] as the main legal act in the sphere was greatly influenced by the Data Protection Directive 1995 as well as the Convention for the Protection of

---

2194 California Consumer Privacy Act of 2018 <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375> accessed 10 May 2020 (CCPA).

2195 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (date of end of validity: 24/05/2018) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046> accessed 10 February 2020.

2196 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) <https://eur-lex.europa.eu/eli/reg/2016/679/oj> accessed 10 February 2020, art 17.

2197 EDPB, Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1): <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf> accessed 10 May 2020.

2198 Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014] <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN> accessed 10 February 2020.

2199 Law 'On Personal Data Protection'.

Individuals with regard to Automatic Processing of Personal Data 1985,[2200] it adopts the respective Right to be Forgotten concept, although with a limited application.

Currently, personal data is to be deleted or destroyed, without the need for a data subject to make a specific request, in the event when:

1) the duration of data storage, determined under the [previously given] consent of a data subject, or under the Privacy Law has expired;

2) legal relations between a data subject, and data controller or processor seized to exist unless otherwise is provided by law;

3) the Ukrainian Parliament Commissioner for Human Rights issued a relevant instruction to do so;

4) a court ruling to remove or destroy personal data has entered into force.[2201]

Additionally, data subject is entitled to the right to make a motivated request, in particular, to destroy his/her personal data to a controller or processor if such data is processed unlawfully as well as to withdraw his/her consent to personal data processing.[2202]

Certain provisions may be further detailed in specific by-laws, for example, processing medical personal data.[2203]

As may be inferred from the provisions mentioned above, particular correspondence to GDPR may still be traced. However, comparatively the scope of application seems to be quite limited indeed. Even though the Ukrainian legislation in force at the time of this Report is likely to include the scope of protection that is boarder, for instance, the right to delete under the CCPA, it still lacks certain coverage aspects as fixed in the Right to be Forgotten under the GDPR.

5.2. Court Cases and Competent Authority Review

So far, several court cases did revolve around the deletion of personal data from information and telecommunication systems.

[2200] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>, accessed 10 February 2020.

[2201] Law 'On Personal Data Protection', art 15, §2.

[2202] ibid, art 8, §2(5), art 11.

[2203] Procedure regarding Electronic Healthcare System Functioning as approved by the Decree of the Cabinet of Ministers of Ukraine 'On Some Aspects of e-Health' as of 2 April 2018 №411 <https://zakon.rada.gov.ua/laws/show/411-2018-п> accessed 10 February 2020.

In the case №577/2983/19, for example, the claimant has pleaded for the erasure of own personal data from the banking database upon closing of his bank account (on ground that legal relations between him as a data subject and a bank as a controller have seised to exist) with claim being denied on the grounds of requirements to retain such information for five more years under the Ukrainian AML legislation.[2204]

In another case №12685/19, the court also rejected the claim pleading to erase personal data, that is personal identification number of claimant's social security file, from all databases on the grounds that since such personal identification number cannot be rejected, therefore, the information about it cannot be deleted.[2205]

As for the competent authority review, the Ukrainian Parliament Commissioner for Human Rights covers the state of the personal data protection in its yearly reports. The Right to be Forgotten was last covered in the report for 2017 where it was reminded that the procedure for executing the right to delete comprises minimal requirements of proper processing of personal data.[2206] In the latest report for 2019 the Commissioner noted that the number of violations of the right to privacy and the Privacy Law in particular has declined over the last year. The right to withdraw consent to personal data processing was, however, said to be one of the most commonly violated rights. The Commissioner has recommended the Cabinet of Minister of Ukraine to take provisions of the Privacy Law into consideration when prototyping, developing, and launching governmental information resources,[2207] although no recommendations to the Parliament of Ukraine to harmonise the Ukrainian privacy legislation with European one have been made.

5.3. Harmonisation with the European Legislation

According to Article 15 of the Ukraine–European Union Association Agreement, Ukraine and the European Union agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the

---

2204 *Case №577/2983/19* (10 November 2019) (Appellate Court of Sumy) <http://reyestr.court.gov.ua/Review/85705627> accessed 10 May 2020.

2205 *Case №12685/19*(11 December 2019) (Second Appellate Administrative Court) <http://reyestr.court.gov.ua/Review/86359546> accessed 10 May 2020.

2206 Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2017 (Secretariat of the Commissioner, 2018) 496 <http://www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf> accessed 10 May 2020 (2018 Yearly Report).

2207 Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in 2019 (Secretariat of the Commissioner, 2020) 194, 200, 201 <http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf> accessed 10 May 2020 (2019 Yearly Report).

highest European and international standards.[2208] Consequently, the Cabinet of Ministers of Ukraine has adopted the Action Plan on the Implementation of the Association Agreement. Ukraine had to improve its personal data legislation by preparing amendments to the Privacy Law to harmonise it with the General Data Protection Regulation including its detailing regarding the Right to be Forgotten.[2209] These amendments should have had to be put in place until 25 May 2018, however no progress was seemingly made.

6. How does your country regulate the liability of internet intermediaries?

Under the Ukrainian law, internet intermediaries are understood as telecom operators (providers), payment infrastructure service operators, registrars (administrators) that assign network identifiers, and other entities that ensure the transmission and storage of information using information and telecommunications systems.[2210]

The Law of Ukraine 'On Electronic Commerce' differentiates three types of legal relations where the liability of internet intermediaries is limited. Thereby, in respect to:

— *electronic transactions* where intermediaries shall not be liable for the content of the information transmitted or received and for potential resulting damage provided that they do not initiate the transmission of such information, select the recipient and cannot change its contents;

— *intermediate (temporary) storage of information* where intermediaries shall not be liable for storing the information and for potential resulting damage provided that they fulfil the conditions of access to and updating information, act promptly to restrict access to information in certain conditions, and do not modify information, interfere with the lawful use of the technology;

2208 Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part <https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf> accessed 10 February 2020 (Association Agreement).

2209 Action Plan on the Implementation of the Association Agreement between the European Union and its Member States, on the one hand, and Ukraine, on the other hand, approved by the Decree of the Cabinet of Ministers as of 25 October 2017 №1106<https://zakon.rada.gov.ua/laws/show/1106-2017-п> accessed 10 February 2020, 11.

2210 The Law of Ukraine 'On Electronic Commerce' 2015 №675-VII <https://zakon.rada.gov.ua/laws/show/675-19> accessed 13 May 2020, art 6, §2 (Law 'On Electronic Commerce').

— *hosting services* where intermediaries shall not be liable for the content of the information transmitted or received and for potential resulting damage provided that they are not aware of any illegal activity concerning such information, and after becoming aware act promptly to remove or restrict access to it.[2211]

Ukraine made the commitment to implement relevant legal rules on the liability of internet intermediaries in the national legislation in the course of association with the EU that stipulates similar liability provisions, although referring to the copyright infringements.[2212] Moreover, the Law 'On Copyright and Related Rights' fixes that hosting service providers shall not be liable for infringement of copyright and (or) related rights, or the consequences of applying take-down measures if they are complaint with certain legal requirements (refer to 0 for take-down notice details).[2213]

Furthermore, the Law 'On Telecommunications' envisages that telecom operators and providers shall not be liable for the content of information that is transmitted through their networks.[2214]

For proposed draft legislation, refer to 0 for more details.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

Legislation on the liability of internet intermediaries will definitely be subject to changes over the next five years. The main tendency which can be observed nowadays is the increase in the liability, creating additional obligations, adopting blocking/filtering mechanism. Right to be forgotten is already implemented to some extent, thus, any definite changes difficult to be predicted.

Current status quo is very likely to be disrupted in the next years. Legislative uncertainty and a lack of particular instruments will soon be eliminated considering efforts to produce complex regulation as described in 2.3. Although the tendency of state regulation is deemed to be very disproportionate, it is balanced out by an active stand of the civil society actors. Private sector players

[2211] ibid, art 9, §4.
[2212] Association Agreement, art 244-248.
[2213] Law 'On Copyright and Related Rights', art 52[2], §2..
[2214] Law 'On Telecommunications', art 40, §4.

are expected to actively advocate for Freedom of Speech and implementing needed instruments of regulation while combating censorship and over-the-top state intervention in the media.

Recent legislative proposals seem to be inclined towards undemocratic limitations where the regulation is scarce. One of the proposed draft laws, aimed at combating disinformation, especially in the conditions of Russian Federation aggression, was criticised by both journalists and the Council on Freedom of Speech and Protection of Journalists to have unjustified limitation of the freedom of speech and rights of journalists. In particular, the ineffectiveness of the proposed criminal sanctions, and excessive and disproportionate administrative sanctions, state interference in the self-regulation of journalists, creation of a new authority aimed at restricting the right to freedom of expression, prohibition of anonymous dissemination of information were cited as the important points for consideration.[2215] This may mean that a strong opposition to the disproportionate proposals by both the civil society and even the state institutions can contribute to the better drafted proposals regulating the freedom of expression.

Some additional rules regarding the liability of internet intermediaries may be inferred from the proposal. In case if it is impossible to determine the author or disseminator of information or information is anonymous, liable is the one who has provided technical possibility for dissemination of information (apparently, the website owner or joint access platform).[2216] Such an approach contradicts the international standards of internet intermediaries' liability in light of holding liable for third-party content which they merely give access to or which they transmit or store.[2217] Such discrepancies with international standards may have quite a negative influence on the media sphere in Ukraine.

2215 'Recommendations of the Council on Freedom of Speech and Protection of Journalists under the President of Ukraine on the Bill on Countering Disinformation' (04 February 2020) <https://detector.media/infospace/article/174473/2020-02-04-rekomendatsii-radi-z-pitan-svobodi-slova-ta-zakhistu-zhurnalistiv-pri-prezidentovi-ukraini-shchodo-zakonoproektu-pro-protidiyu-dezinformatsii/> accessed 10 May 2020.

2216 'Comparative table to the Draft Law of Ukraine 'On making amendments to certain legislative acts of Ukraine on ensuring national informational security and right of access to reliable information' <https://detector.media/infospace/article/174057/2020-01-21-porivnyalna-tablitsya-do-proektu-zakonu-ukraini-pro-vnesennya-zmin-do-deyakikh-zakonodavchikh-aktiv-ukraini-shchodo-zabezpechennya-natsionalnoi-informatsiinoi-bezpeki-ta-prava-na-dostup-do-dostovirnoi-informatsii/> accessed 16 February 2020, art 54 para 2.

2217 Appendix to Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14> accessed 15 February 2020, art 1 para 1.3.7.

An example of the active counteraction of the civil society can be seen in the reaction to the liability of internet intermediaries in light of the Draft Law 'On Media'. During the public discussion of the liability limitations the representatives of the service provider associations stressed the importance of redlining the proper limits. In particular, enforcing content blocking using administrative and technical instruments of pressure without a court ruling was stressed. It was also suggested to remove telecom operators and providers from the list of subjects to enforce blocking due to technical constraints. At the same time, experts emphasise that the proposed mechanism of blocking corresponds to the requirements of Manilla Principles and the ECJ case law. On the contrary, experts highlight that the current wording may potentially be disproportionate and create unnecessary consequences. This may as well be another attempt to strengthen government control over media (refer to 2.3).

Another attempt to meddle with the liability limitation under the Draft Law 'On Gambling' was also similarly criticised. Experts once again stressed the technical inability for telecom operators and providers to enforce access blocking (refer to 2.3).

One of the dimensions of a successful European integration of Ukraine is maintaining proper checks and balances when drafting the laws to guarantee the necessary level of freedom of speech protection grounded on the best practices of the European law. Especially when it comes to the regulation of the civil society sector. In Europe, decentralisation in the form of strengthening the role of professional associations and self-regulation of certain spheres is increasing. Therefore, the legislation should be more balanced in order to protect fundamental elements of the Freedom of Expression, especially in the online environment. This requires establishing balanced instruments that can be enforced by state authorities and mechanisms for court protection.

The professional community should develop effective mechanisms for extra-judicial protection through: 1) resolving grievance mechanisms; 2) appealing against actions of providers and other market participants in case of illegal blocking; 3) imposing sanctions for illegal actions by the professional community itself.

When it comes to the Right to be Forgotten, although Ukrainian legislation covers some aspects, the grounds on which personal data can be deleted do not fully correspond to the European practice. The scope of the right to delete is much narrower than that of the Right to be Forgotten as fixed in the GDPR. Ukraine does, however, plan to harmonise its privacy legislation with the EU's

one, meaning it is reasonable to expect developments in this field that will ensure better mechanisms for data subject's rights protection.

It is possible to assume the following perspectives of the development of legislation regarding the liability of internet intermediaries over the next five years:

1. The tendency of increasing the liability on internet intermediaries, including the social media networks, may be observed. This can be explained by the necessity to fight against hate speech, disinformation and illegal content in the digital environment. Also, more additional obligations will be potentially imposed on intermediaries. For instance, the 'joint access platforms' (that is, social media) may be obligated to acquaint users with the platform use policy, fulfil certain requirements of copyright law, verify user's age, or establish an effective instrument for forwarding complaints.[2218] There are particular pending questions so as to which intermediaries will be affected though.

2. Correspondingly, the adoption of certain blocking/filtering measures is expected. The increase of the liability of internet intermediaries goes hand in hand with the creation of a mechanism to enforce blocking/filtering via administrative instruments. However, the opposition from the civil society is clearly visible to influence such by suggesting court review to implement such measures.

3. Among other possible legislative perspectives in this area, it is worth mentioning the adoption of the co-regulation model. Such model of legal regulation may include the establishment of the new competent body which will be empowered to interact with the joint access platforms providers by means of concluding special agreements with them (for example, in the form of memorandums of cooperation). The above mentioned agreements may envisage the obligation for providers to establish in the terms of use the prohibition to share certain types of content, to cooperate with state authorities by necessity. Such practice has already been adopted in France: since November 2018 Facebook cooperates with local authorities on the issues of hate speech, and even provides information at the request of judicial bodies since June 2019.[2219]

4. Personal data protection legislation is likely to be harmonised with the European standards which will respectively influence the right to be forgotten.

[2218] Draft Law 'On Media' №2693 <https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812>, accessed 16 February 2020, art 23.

[2219] French Gov't Says Facebook Has Agreed to Provide IP Addresses to Help Counter Online Hate <https://www.cnsnews.com/news/article/fay-al-benhassain/french-govt-says-facebook-has-agreed-provide-ip-addresses-help> accessed 17 February 2020.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

8.1. Legal Overview

Currently, the regulation on hate speech may be deemed to be scarce. It is criticised for the lack of distinction between soft and hard hate speech highlighting that hate speech is only punishable under the criminal law,[2220] and vague provisions.[2221]

The main framework is set in:

— The Constitution which establishes a discrimination prohibition standard and prohibition on the creation and functioning of political parties and non-governmental organisations, goals or activities of which are aimed at inciting ethnic, racial, religious hatred.[2222]

— The Law 'On the Principles of Prevention and Combating Discrimination in Ukraine'[2223] which further details mechanism and framework for non-discrimination.

— The Law 'On Information' which fixes, in particular, '*incitement of interethnic, racial, religious hatred*' as a part of the protection against the misuse of the right to information rule.[2224]

— The Law 'On Television and Radio Broadcasting' which fixes, in particular, '*incitement of national, racial or religious hostility and hatred*' as a part of the protection against the abuse of broadcasting organisations activity freedom rule and the prohibition of such actions as well as 'their positive presentation (interpretation)' as a part of the state policy.[2225]

— Criminal Code which recognises, in particular, 'incitement to national, racial or religious hostility and hatred or to humiliate national honour

[2220] Human Rights Online: Agenda for Ukraine, 32.
[2221] Maryna Dorosh, 'Hate speech - new manifestations and consequences' (2015) <https://ms.detector.media/zakonodavstvo/post/12829/2015-03-17-mova-vorozhnechi-novi-proyavi-ta-naslidki/> accessed 03 May 2020.
[2222] Constitution of Ukraine art 24, §2, art 37, §1.
[2223] The Law of Ukraine 'On the Principles of Prevention and Combating Discrimination in Ukraine' 2012 №5207-VI <https://zakon.rada.gov.ua/laws/show/5207-17> accessed 14 February 2020.
[2224] Law 'On Information', art 28.
[2225] Law 'On Television and Radio Broadcasting', art 6, §2(4), art 4(7).

> and dignity or the image of feelings of citizens in connection with their religious beliefs' as a punishable act.[2226]

The regulation of hate speech may be considered to be somewhat shallow and inconsistent in the framework of national legislation. Experts stressed that the constitutional protection is 'extremely broad', while the regulation in the laws extends to different types of speech, not only hate speech *per se*, which creates difficulties in the application of protection standards.[2227]

8.2. Court and Law Enforcement Issues

Court cases statistics seems to reflect a low interest in application of the rules against hate speech. According to the consolidated official judiciary statistics, during 2006–2019 a total of 33 criminal court cases regarding art 161 of the Criminal Code of Ukraine were considered with six more pending in 2020.[2228] Only in 18 cases a court reached a verdict (including four with reconciliation).[2229] The rest were returned, dismissed, or closed. Only in one instance the court reached a decision to apply measures of medical treatment. Considering the online environment, during 2007–2018 only 3 out of 14 cases dealt with dissemination of illegal content on the Internet. The Digital Rights Agenda for Ukraine Report highlights that 'typical of these decisions is the lack of an attempt of the courts to analyse the content of common statements on their own, not to mention the application of the practice of the European Court of Human Rights and the Perinçek test. In most cases the courts blindly rely on the conclusions of the expert examination and do not give them their own assessment.'[2230] This statement is also supported by the Freedom of Expression Analytical Report,[2231] which details that the courts do not independently analyse the alleged hate speech, how it impacts potential auditoriums depending on its size in the social media, or the nature of the disseminated content (repost, comment, hyperlinks etc.)

2226 Criminal Code of Ukraine, art 161, §1.

2227 OSCE, 'Comparative Legal Analysis of Ukrainian Regulation of Hate Speech in the Media' (2018) 1, 2 <https://www.osce.org/fom/371841?download=true> accessed 03 May 2020.

2228 State Court Administration, Official website (2020) <https://court.gov.ua/inshe/sudova_statystyka/>accessed 1 May 2020.

2229 When declaring a verdict on a general basis, a court independently examines the circumstances of a case and decides on a punishment. If there is a verdict on the grounds of the agreement for reconciliation, then the court checks such an agreement for compliance with the requirements of the criminal material and procedural regulation and whether it violates public order, approves the agreement and appoints the punishment decided upon by the parties to the agreement.

2230 Human Rights Online: Agenda for Ukraine.

2231 L. Opryshko, V. Volodovska, M. Drovovyi, 'Freedom of Expression on the Internet: Legislative Initiatives and Practice of Examination of Criminal Cases in Ukraine in 2014-2018' (2019) <https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf> accessed 14 February 2020.

Furthermore, it is worthwhile to pay attention to the quality of police investigation. Consolidated criminal offences statistics published by the Prosecutor General's Office shows that in the span of 2013–2019 there were only 372 crimes alleging Article161 of the Criminal Code of Ukraine.[2232] This constitutes as little as 0.01% in relation to the total amount of registered crimes (3 705 659 crimes) within the same timeframe. Furthermore, only in 32 cases alleged suspects were identified. To make it worse, only seven allegedly committed crime cases were further transferred for court hearing with an indictment. The access to the Unified Register of Pre-Trial Investigations is restricted to the general public, thus making the cases impossible to analyse further. The statistics makes it safe to assume that the crime rate of the cases under art 161 of the Criminal Code seems to be drastically small in comparison. Moreover, human rights protection groups often report ineffectiveness of the police investigation,[2233] especially regarding hate crimes. Human Rights Watch together with several more organisations sent a Joint Letter[2234] to the Ministry of Internal Affairs and Prosecutor General addressing violent attacks against LGBT, women's rights activists, human rights defenders and journalists by radical groups in several Ukrainian cities. The letter addresses, in particular, the lack of appropriate response of the law enforcement bodies and reluctance to either initiate investigations, or apply effective measures. This also concerns the cases where the alleged attackers claimed the responsibility online. In general, policing is seen to be quite ineffective in this area.[2235]

8.3. Live Broadcasting and YouTube

The main authority in the area, the National Council Television and Radio of Ukraine, can enforce administrative sanctions against broadcasting organisations for the breach of the said Law for the violation of anti-hate speech regulations.[2236] Most recently, the Council issued a Decision fixing numerous alleged hate speech instances between August 2019 and December 2019 during the '112 Ukraine' channel live broadcasting in the speeches of several studio guests, among which were the ex- and current members of the Ukrainian

[2232] Prosecutor General's Office of Ukraine (2020) <https://old.gp.gov.ua/ua/stst2011.html> accessed 16 February 2020.

[2233] Amnesty International, 'Ukraine: A year after attack on Roma camp in Kyiv, no justice for victims' (2019) <https://www.amnesty.org/en/latest/news/2019/04/ukraine-a-year-after-attack-on-roma-camp-in-kyiv-no-justice-for-victims/> accessed 15 February 2020.

[2234] Human Rights Watch, 'Joint Letter to Ukraine's Minister of Interior Affairs and Prosecutor General Concerning Radical Groups' (2018) <https://www.hrw.org/news/2018/06/14/joint-letter-ukraines-minister-interior-affairs-and-prosecutor-general-concerning> accessed 16 February 2020.

[2235] Human Rights Watch, 'Ukraine. Event of 2019' (2020) <https://www.hrw.org/world-report/2020/country-chapters/ukraine> accessed 16 February 2020.

[2236] Law 'On Television and Radio Broadcasting', art 72.

Parliament.[2237] The Council states that the provisions of the Laws 'On Information' (Article 28(1)) and 'On Television and Radio Broadcasting' were breached in the context of calls for starting an aggressive war or propaganda of such, and/or incitement of national, racial or religious hostility and hatred (Article 6(2)(iv)) and the promotion or propaganda of the authorities of the aggressor State and their individual actions justifying or recognising the legitimate occupation of the territory of Ukraine (Article (6)(2)(ix)). Further audit is to follow. On the contrary, the '112 Ukraine' channel disapproves the alleged violations stating that such interpretation constitutes the freedom of speech violation and can be deemed as censorship. The channel further claims that the said commentaries were made by the studio guests and do not represent its own opinions.[2238]

Furthermore, the Council has already fined several broadcasting organisations for hate speech violations. For example, 'Maksi-TV' broadcasting was recognised to allow the dissemination of unobjective information, unaugmented accusations, and the usage of narrative similar to Russian propaganda by a studio guest, who happened to be ex-Prime Minister of Ukraine.[2239] Interestingly enough, the Council notes that there were no active attempts from the presenter to change the rhetoric of the studio guest, stop or interfere with the statements, the content of which violates anti-hate speech regulation. The opposite point of view or signs of discussion of the issues during the broadcast were not presented, which violates viewers' right to objective information and abuse of the TV broadcasting Right to Freedom of Expression in the Council's mind.

The Council in general has been quite active also fining several channels for the breach of the aforementioned regulation.[2240]

It is important to discuss these alleged violations since TV broadcasters publish the recordings of live broadcasts on YouTube allowing for possible further

---

[2237] Decision On the appointment of unscheduled on-site inspection of LLC 'TRK '112-TV' №15 as of 09 January 2020 <https://www.nrada.gov.ua/wp-content/uploads/2020/01/R-2020-00015.pdf> accessed 23 February 2020.

[2238] '112 Ukraine' statement on the next fact of censorship by the National Council of Ukraine on Television and Radio' (09 January 2020) <https://tv-ua.112.ua/novyny-kanalu/zaiava-112-ukraina-z-pryvodu-cherhovoho-faktu-tsenzury-z-boku-natsrady-z-tb-521342.html> accessed 23 February 2020.

[2239] 'Maxi-TV is subject to sanctions of 'warning' and 'fine' in the amount of more than one hundred thousand hryvnias for the spread of hate speech' (09 January 2020) <https://www.nrada.gov.ua/telekompaniyi-maksi-tv-zastosovano-sanktsiyi-ogoloshennya-poperedzhennya-ta-styagnennya-shtrafu-v-sumi-ponad-sto-tysyach-gryven-za-poshyrennya-movy-vorozhnechi/> accessed 23 February 2020.

[2240] 'NewsOne should pay over UAH 95,000 for hate speech' (07 February 2019) <https://www.nrada.gov.ua/telekanal-newsone-povynen-splatyty-shtraf/> accessed 23 February 2020.

dissemination of hate speech. Under the Rabat Plan of Action,[2241] a six-part threshold test was proposed to determine the severity of the hate speech expressions: Context, Speaker, Intent, Content and form, Extent of the speech act and Likelihood. The key elements in this regard are Context, Speaker, and Extent. While the application of first two may be regarded as reaching the threshold enough to claim the hate speech violation, it is the Extent feature that plays an important role in the analysis. Since the recordings are accessible for the general public though YouTube, they are an active source of the alleged hate speech dissemination.

8.4. Other Implications

In the course of the war conflict in the Eastern Ukraine and Crimea it is important to focus on the state of hate speech in that context as well. Tendencies are reflecting the disproportionate rise of hate speech instances towards the whole Russian population as well as the residents of the temporary occupied territories accusing them of the current state of affairs. In such regard the state authorities have been criticised for the lack of a unified state policy that allows the abuse of free speech.[2242] Ukrainian mass media are claimed to have no consistent editorial practices and even a complete disregard of journalistic standards.[2243] On the other side, the analysis of the online media in the separate regions of Donetsk and Lugansk districts as well as Crimea leads to a conclusion that distinct presence of hate speech toward the Ukrainian population is noted.[2244]

8.5. Recommendations

As it seems, hate speech regulation generally produces inconsistent results. While the legislation is scarce and deserves improvement, law enforcement does not provide adequate solutions as well. Essentially, the balance tends to shift more in favour of the freedom of speech which results in the absence of real barriers

---

[2241] Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (2013) <https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf> accessed 23 February 2020.

[2242] A. Blaha, O. Martynenko, B. Mois, R. Shutov, 'Freedom of speech in times of information warfare and armed conflict' (2017) <https://helsinki.org.ua/wp-content/uploads/2018/01/Web_Svoboda_Slova_A5_Ukr3.pdf> accessed 24 February 2020.

[2243] Tetiana Bondarenko, 'Hate speech: how the Ukrainian media neglects journalistic standards' (2017) <http://detector.media/infospace/article/128539/2017-07-05-mova-vorozhnechi-yak-ukrainski-zmi-nekhtuyut-zhurnalistskimi-standartami/> accessed 22 February 2020.

[2244] Institute of Mass Information, 'Analysis of the so-called mass media of 'DNR' and 'LNR': in every tenth piece of news – hate speech towards Ukrainians, 11% of news are fakes' (2017) <https://imi.org.ua/news/analiz-internet-zmi-tzv-dnr-ta-lnr-u-kojniy-desyatiy-novini-mova-vorojnechi-schodo-ukrajintsiv-11-i17084> accessed 22 February 2020.

for hate speech restrictions. The main recommendation lies in between the lines of improving legislation and establishing a state-wide policy regarding hate speech.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

In the course of answer to this question, a brief analysis of the balance between the freedom of speech online and privacy will be made.

The Constitution of Ukraine protects the right to privacy though (i) prohibiting unlawful interference in private and family life, (ii) and collection, storage, use and dissemination of confidential information about an individual without his/her consent. It further allows to (iii) familiarise with information about themselves available with state authorities unless such is protected by law and (iv) guarantees judicial protection of the right to refute inaccurate information and (v) the right to demand the removal of any information.[2245] The Right to Freedom of Speech and the Right to Privacy have the same value and are equally protected under the Constitution of Ukraine. Experts highlight that in cases where there is a need to disclose information that falls within the scope of a person's private life, a balance must be struck between these rights.[2246]

Information about a person is a source of possible danger to his/her privacy. Due to the openness of the Internet and its peculiarity as a system that can collect and process information about a person, the issue of privacy is extremely important when using the communication capabilities of this global network. The exchange of thoughts via the Internet is fundamentally different from usual means of communication. The electronic message, moving in a network, passes step by step, from one operator to another, choosing the most optimum of ways. Each of the operators acts as an intermediate link and has the opportunity to intervene in this process. Operators can not only learn about the content of the message, but also additional information. At the same time, in most cases, a person has no idea what personal information is and for what purpose it is collected and processed.[2247]

[2245] Constitution of Ukraine, art 32.

[2246] 'Which right has priority: the right to freedom of speech or the right to privacy?' <https://www.ppl.org.ua/bibliotech/2-2> accessed 19 May 2020.

[2247] Andrii Paziuk 'Privacy and the Internet' <http://khpg.org/index.php?id=968016432> accessed 19 May 2020.

Solving the issue of protecting the privacy of Internet users and Freedom of Expression online is possible with a set of measures, organisational and technical.

First of all, at the organisational level it is necessary to ensure the rights online, Ukraine must enact legislation that will protect a person's privacy online. The right to privacy also requires legislative mechanisms to protect against damage to a person's reputation through the dissemination of inaccurate information online. An equally important element is the freedom from undue surveillance and intrusion into the secrecy of correspondence and electronic communications - security measures and online restrictions must meet international standards. This means, in particular, that Ukraine should not provide law enforcement agencies with uncontrolled opportunities for direct access to the Internet. The anonymity of the Internet user should be ensured as one of the essential principles, which allows to guarantee a certain level of privacy when expressing views online. On the other hand, it is fair to say that the principle of anonymity, which avoids identification, is not always in the public interest. Such as the fight against illegal and harmful content on the Internet, financial fraud or copyright infringement.

The phenomenon of the Internet requires that adequate measures be taken to ensure the proper functioning of the Right to Freedom of Expression online, along with other human rights.

10. How do you rank the access to freedom of expression online in your country?

Freedom of expression	Online media regulation	Internet censorship regulation and case law	**Band score**
3	2	4	**3**

Freedom of Expression. Despite having established constitutional guarantees for the freedom of expression, in particular in certain aspects of online environment, the applicability of said guarantees desires improvement. Ukrainian Parliament Commissioner for Human Rights in her latest Report notes that there have been 243 Freedom of Expression violations in Ukraine in 2019,[2248] 172 of which have been physical aggression against journalists. In total, this is only 1 act of

[2248] 2019 Yearly Report, 223.

aggression less than last year.[2249] On top of that, international analytic sources rank the state of freedom of speech in Ukraine quite low. Reporters Without Borders lists Ukraine at №96 (out of 180 countries) in World Press Rating Index highlighting 'access to information, news manipulation, violations of the confidentiality of sources, cyber-attacks, and excesses in the fight against fake news (including a proposed anti-disinformation law that would threaten press freedom)' as the main concerns.[2250] Freedom House ranked Ukraine at №31-33 together with Singapore and Uganda (out of 65 countries) in its Freedom of the Net Report highlighting partly censored information landscape, efforts by political actors to manipulate debates through disinformation and paid content, persistent cyberattacks.[2251] Most notably, the state has enforced a nation-wide blocking of a number of Russian websites under the notorious Decree of the President of Ukraine №133/2017 (refer to 3.1).[2252]

Overall, we rank the Freedom of Expression 3 out of 5.

Online Media Regulation. Ukraine has put in place a considerable number of laws regulating technology, media, and telecommunication industry, including various laws on media. However, the legislation rarely addresses online media in particular, as it generally focuses on traditional media. Regulation in force distinctly lacks particular provisions necessary for setting clear and transparent ground for online media activity. In particular cases related to content blocking or filtering, the lack of implementation mechanisms renders the implementation quite difficult. The absence of online media regulation may lead to a situation where online media creators, including journalists, may be restricted in enjoying the needed level of constitutional protection. The proposed regulation as described in 2.3 was criticised for potentially setting the ground for unchecked state interference and censorship.

Since these flaws in the Ukrainian legislation are rather substantial, we rank the online media regulation 2 out of 5.

Internet Censorship and Case Law. Even though the law guarantees the prohibition of censorship, it was highly stressed that the absence of clear regulation leads to imbalanced practice. Court cases usually focus on the defamation matters, where claims are directed at the protection of one's reputation rather than imposing

[2249] 2018 Yearly Report, 116.
[2250] Reporters without borders, 'Ukraine' (2019) <https://rsf.org/en/ukraine> accessed 18 February 2020.
[2251] Freedom of the Net Report 2019 <https://freedomhouse.org/country/ukraine/freedom-net/2019> accessed 20 May 2020.
[2252] Freedom House, 'Should Ukraine Drop Sanctions against Russian Tech Companies?' <https://freedomhouse.org/report/policy-brief/2019/should-ukraine-drop-sanctions-against-russian-tech-companies>, accessed 14 May 2020.

censorship. However, this shows a general insignificance of challenging censorship in court.

Based on that, we find the Internet censorship regulation and case law can be ranked as 3 out of 5.

Band Score. With a band score of 3 out of 5, it can be concluded that Ukraine has noticeable inefficiencies in the regulation of freedom of speech online, mainly coming from the lack of area-focused laws that would have regulated most freedom of speech online-related matters.

11. How do you overall assess the legal situation in your country regarding internet censorship?

ELSA Ukraine's findings regarding the state of the internet censorship and related issues in Ukraine can be summarised as follows:

1. **Freedom of speech** legislation at the time of writing of this Report does not sufficiently covers online environment aspects. Instead, the regulation is revolving around mostly traditional media. However, such limitation does not preclude the legislation in force to be applied online.
2. **Censorship** is clearly defined and widely prohibited. However, it is stressed that the regulation deserves more improvement in order to provide for anti-abuse of state powers.
3. The **Right to Information** has a clear definition and enjoys protection. At the same time, mismatches and unclear provisions in the legislation are noticed. Overall, the legislation seems to be intransparent and overloaded.
4. **Blocking and taking down** of internet content is regulated to some extent. Although, there is no general instrument allowing such measure, certain sectoral laws contain specific provision. Such include (i) martial and emergency situations laws regarding content blocking in extraordinary situations, (ii) Civil Code that foresees filtering measures applicable in instances of individual rights' breaches, (iii) Criminal Code that targets pornographic content, (iv) broadcasting and cinematography laws which prohibit certain content, (v) telecommunications law that sets an obligation for telecom providers to enforce child pornography blocking, (vi) copyright protection law that sets a takedown procedure for relevant copyright violations. At the

same time, it is noted that generally the regulation does not provide for the implementation mechanism of blocking and takedown measures.

5. A couple of **policy papers** aimed at information security attempt to lay down a framework for blocking and takedown related regulation in light of, in particular, the aggression from the Russian Federation and hybrid war. However, the policy papers were criticised for vague provisions and the lack of actual outcome.

6. In recent year there have been quite a few **legislation proposals**. Most noticeably among the others, the proposed regulation was aimed at blocking and takedown of internet content. The draft legislation was criticised to be imbalanced and allowing for excessive state inference.

7. Among the analysed **grounds** for internet content blocking, the purposes of national security and integrity stand out the most. In particular, several Russian websites were blocked by imposing sanctions. Although, the analysed legislative grounds seem to suggest a breach of due process. At the same time, the blocking was scrutinised by the Ukrainian court and proved to be necessary in democratic society.

8. Unlawful content in **civil law** and illegal content in **criminal law** are treated somewhat differently. Whereas civil law establishes a wide range of restricted content, criminal law is limited only to pornographic content.

9. There is indeed a **context** in Ukraine which details that otherwise legal content is blocked or filtered. Such may include the promotion and propaganda that justifies the legitimate occupation of the territory of Ukraine by the Russian Federation.

10. **Judicial review** seems to be quite shallow regarding the analysis of the freedom of speech breaches. In this regard, there have been no landmark court rulings. The court review was also criticised for being shallow and incomprehensive. Breaches of due process in criminal proceedings were noticed.

11. The legislation *per se* corresponds to the **requirements set out in the ECHR case law** to a certain extent. While the criteria for content blocking or filtering are fairly clearly prescribed by the law, some flaws are noticeable. For example, the criterion of the necessity in the democratic society as a part of the three conditions test is not

prescribed in the legislation. Certain ambiguousness of the law may lead to the disproportionate measures of application.

12. Blocking and taking down of internet content is scarcely **self-regulated** in Ukraine. Even though, several policy documents created by the private law actors do exist, their applicability comes unnoticed. At the same time, civil society tends to create a very noticeable counteraction with regards to governmental proposals for further regulation.

13. Ukraine adopts the '**Right to be Forgotten**' concept that fairly corresponds to the requirements as set out in the GDPR. However, it still needs to provide certain more aspects to be covered.

14. The **liability of internet intermediaries** is scarcely regulated in Ukraine. Generally, telecom operator and providers are not liable for the content of information they transmit. The only directly applicable provisions are used in the e-commerce, where internet intermediaries may be liable for information transmitted if specific conditions are met.

15. The adequate balance between allowing freedom of speech online and protecting against **hate speech** seems not to be reached. The legislation does not provide exhaustive criteria to define hate speech, therefore it may lead to the disproportionality in the application of restrictive measures.

Conclusion

Overall, legal situation regarding Freedom of Expression online is vastly unregulated. Most noticeably, legislation approaches the definition of content that may be filtered or blocked somewhat differently. This may lead to discrepancies in practical application of the law in different spheres. Legislative proposals seem to target this and many other issues by attempting to introduce a complex law that will create ramifications for the mass media behaviour, including online aspects, irrespective of a medium in question. However, such were criticised for allowing a potential disproportionate state interference. Whereas experts stress the presence of state interference via indirect censorship despite fully-encompassing censorship prohibition, and the attempts to introduce legislation aimed at extending state power over the media and particular blocking and takedown measures without a need for a court ruling, it is highly desirable to point the attention to the probability of excessive and imbalanced regulation. It is definitely true that it is high time to introduce the necessary regulation in order to provide for clear and understandable criteria and measures of, in particular, various blocking and takedown instruments. At the same time an adequate balance in the regulation must be reached so as not to create further discrepancies.

Table of legislation

Provision in Ukrainian language	**Corresponding translation in English**
Частина 3 статті 15 Конституції України: Цензура заборонена.	Part 3 of the Article 15 of the Constitution of Ukraine: Censorship is forbidden.
Частина 2 статті 24 Конституції України: Рівність прав жінки і чоловіка забезпечується: наданням жінкам рівних з чоловіками можливостей у громадсько-політичній і культурній діяльності, у здобутті освіти і професійній підготовці, у праці та винагороді за неї; спеціальними заходами щодо охорони праці і здоров'я жінок, встановленням пенсійних пільг; створенням умов, які дають жінкам можливість поєднувати працю з материнством; правовим захистом, матеріальною і моральною підтримкою материнства і дитинства, включаючи надання оплачуваних відпусток та інших пільг вагітним жінкам і матерям.	Part 2 of the Article 24 of the Constitution of Ukraine: Equality of rights of women and men is ensured by: providing women with equal opportunities with men in socio-political and cultural activities, in education and training, in work and remuneration for it; special measures for the protection of women's health and health, the establishment of pension benefits; creating conditions that enable women to combine work with motherhood; legal protection, material and moral support of motherhood and childhood, including the provision of paid leave and other benefits to pregnant women and mothers.
Стаття 32 Конституції України: Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.	Article 32 of the Constitution of Ukraine: The collection, storage, use and dissemination of confidential information about a person without his or her consent is not permitted, except in cases specified by law and only in the interests of national security, economic well-being and human rights. Every citizen has the right to get acquainted with information about himself in public authorities, local governments, institutions and organisations, which is not a state or other secret protected by law. Everyone is guaranteed judicial protection of the right to refute inaccurate information about themselves and their family members and the right to demand the removal of any information, as well as the right to compensation for material and moral damage caused by the collection, storage, use and dissemination of such inaccurate information.
Стаття 34 Конституції України: Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати	Article 34 of the Constitution of Ukraine: Everyone is guaranteed the right to freedom of thought and speech, and to the free expression of his or her views and beliefs. Everyone has the right to freely collect, store, use and disseminate information by

інформацію усно, письмово або в інший спосіб - на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.	oral, written or other means of his or her choice. The exercise of these rights may be restricted by law in the interests of national security, territorial indivisibility or public order, with the purpose of preventing disturbances or crimes, protecting the health of the population, the reputation or rights of other persons, preventing the disclosure of information received confidentially, or supporting the authority and impartiality of justice.
Стаття 277 Цивільного кодексу України: 1. Фізична особа, особисті немайнові права якої порушено внаслідок поширення про неї та (або) членів її сім'ї недостовірної інформації, має право на відповідь, а також на спростування цієї інформації. 6. Фізична особа, особисті немайнові права якої порушено у друкованих або інших засобах масової інформації, має право на відповідь, а також на спростування недостовірної інформації у тому ж засобі масової інформації в порядку, встановленому законом. Якщо відповідь та спростування у тому ж засобі масової інформації є неможливими у зв'язку з його припиненням, така відповідь та спростування мають бути оприлюднені в іншому засобі масової інформації, за рахунок особи, яка поширила недостовірну інформацію. Спростування недостовірної інформації здійснюється незалежно від вини особи, яка її поширила. 7. Спростування недостовірної інформації здійснюється у такий же спосіб, у який вона була поширена.	Article 277 of the Civil Code of Ukraine: 1. Individual, whose personal incorporate rights have been violated due to a distribution of false information about them and (or) their family members, has a right of reply as well as a right to demand confutation of this information. 6. Individual, whose personal incorporate rights have been violated in printed other kinds of media outlets has a right of reply as well as a right to demand confutation of this information in the same media outlet according to the order prescribed by law. If a reply and confutation in the same media outlet is impossible due to its shut down, such a reply and confutation must be divulged in another media outlet. Expenses must be covered by those, who distributed false information. Confutation of false information is provided regardless of a distributor's guilt. 7.Confutation of false information is carried out in the same manner as it was distributed.
Стаття 278 Цивільного кодексу України: 1. Якщо особисте немайнове право фізичної особи порушене у газеті, книзі, кінофільмі, теле-, радіопередачі тощо, які готуються до випуску у світ, суд може заборонити розповсюдження відповідної інформації. 2. Якщо особисте немайнове право фізичної особи порушене в номері (випуску) газети, книзі, кінофільмі, теле-, радіопередачі тощо, які випущені у світ, суд може заборонити (припинити) їх	Article 278 of the Civil Code of Ukraine: 1. If an infringement of a personal incorporeal right is found in a newspaper, book, film product, TV or radio programme etc., which are about to be made public, the court can prohibit the distribution of this information. 2. If an infringement of a personal incorporeal right is found in a newspaper issue, book, film product, TV or radio programme etc., which have already been made public, the court can prohibit (put on

розповсюдження до усунення цього порушення, а якщо усунення порушення неможливе, - вилучити тираж газети, книги тощо з метою його знищення.	hold) the distribution of this information until the violation is removed. If it is not possible remove the violation the court can expropriate the issue of a newspaper, book etc. to subject it to the further destruction.
Стаття 279 Цивільного кодексу України: 1. Якщо особа, яку суд зобов'язав вчинити відповідні дії для усунення порушення особистого немайнового права, ухиляється від виконання судового рішення, на неї може бути накладено штраф відповідно до Цивільного процесуального кодексу України. 2. Сплата штрафу не звільняє особу від обов'язку виконати рішення суду.	Article 279 of the Civil Code of Ukraine: 1. If a person, who is obliged by the court to take certain actions in order to remove a violation of the personal incorporeal right, eludes execution of judgment, a fine can be imposed in accordance with the Civil Procedural Code of Ukraine. 2. Payment of the fine does not release from the obligation to execute a reasonable judgment.
Стаття 297 Цивільного кодексу України: 1. Кожен має право на повагу до його гідності та честі. 2. Гідність та честь фізичної особи є недоторканними. 3. Фізична особа має право звернутися до суду з позовом про захист її гідності та честі.	Article 297 of the Civil Code of Ukraine: 1. Everyone has a right to respect for honour and dignity. 2. Honour and dignity of an individual are indefeasible. 3. Individual has a right to lodge an appeal to the court asking for protection of their honour and dignity.
Стаття 298 Цивільного кодексу України: 1.Фізична особа має право на недоторканність своєї ділової репутації. 2.Фізична особа може звернутися до суду з позовом про захист своєї ділової репутації.	Article 298 of the Civil Code of Ukraine: 1.Individual has a right to inviolability of their business reputation. 2.Individual has a right to lodge an appeal to the court asking for protection of their business reputation.
Стаття 299 Цивільного кодексу України: Фізична особа має право на недоторканність своєї ділової репутації. Фізична особа може звернутися до суду з позовом про захист своєї ділової репутації.	Article 299 of the Civil Code of Ukraine: A natural person shall have the right to inviolability of his/her goodwill. A natural person may apply to the court with a claim for protection of his/her goodwill.

Частина 2 статті 309 Цивільного кодексу України : 2.Цензура процесу творчості та результатів творчої діяльності не допускається.	Part 2 of the Article 309 of the Civil Code of Ukraine: 2.The censorship of the process of creativity and the results of creative activity should not be allowed.
Стаття 301 Цивільного кодексу України: 1.Фізична особа має право на особисте життя. 2.Фізична особа сама визначає своє особисте життя і можливість ознайомлення з ним інших осіб. 3.Фізична особа має право на збереження у таємниці обставин свого особистого життя. 4.Обставини особистого життя фізичної особи можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що підтверджено рішенням суду, а також за її згодою.	Article 301 of the Civil Code of Ukraine: 1.Individual has a right to private life. 2.Individual determines their private life and a possibility of others to familiarise with it independently. 3. Individual has a right to keep the circumstances of their private life secret. 4.Circumstances of the individual private life can be made public only if they comprise elements of crime which are avowed by the court or on the ground of a consent of the individual.
Стаття 862 Цивільного кодексу України: 1. Якщо сторона у договорі підряду внаслідок виконання договору одержала від другої сторони інформацію про нові рішення і технічні знання, у тому числі й такі, що не захищаються законом, а також відомості, що можуть розглядатися як комерційна таємниця, вона не має права повідомляти їх іншим особам без згоди другої сторони.	Article 862 of the Civil Code of Ukraine: 1. If a party to a contract has received information about new decisions and technical knowledge from the other party as a result of performance of the contract, including information not protected by law, as well as information that may be considered a trade secret, it shall not have the right to disclose it. to other persons without the consent of the other party.
Стаття 895 Цивільного кодексу України: 1. Виконавець і замовник зобов'язані забезпечити конфіденційність відомостей щодо предмета договору на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, ходу його виконання та одержаних результатів, якщо інше не встановлено договором. Обсяг відомостей, що належать до конфіденційних, встановлюється договором.	Article 895 of the Civil Code of Ukraine: 1. The Contractor and the Customer are obliged to ensure the confidentiality of information on the subject of the contract for the performance of research or development and technological work, the progress of its implementation and the results obtained, unless otherwise provided by the contract. The amount of information belonging to confidential information is established by the agreement.

Стаття 1121 Цивільного кодексу України: 1. З урахуванням характеру та особливостей діяльності, що здійснюється користувачем за договором комерційної концесії, користувач зобов'язаний: 1) використовуватиторговельну марку та інші позначення правоволодільця визначеним у договорі способом; 2) забезпечити відповідність якості товарів (робіт, послуг), що виробляються (виконуються, надаються) відповідно до договору комерційної концесії, якості аналогічних товарів (робіт, послуг), що виробляються (виконуються, надаються) правоволодільцем; 3)дотримуватися інструкцій та вказівок правоволодільця, спрямованих на забезпечення відповідності характеру, способів та умов використання комплексу наданих прав використанню цих прав правоволодільцем; 4) надавати покупцям (замовникам) додаткові послуги, на які вони могли б розраховувати, купуючи (замовляючи) товари (роботи, послуги) безпосередньо у правоволодільця; 5) інформувати покупців (замовників) найбільш очевидним для них способом про використання ним торговельної марки та інших позначень правоволодільця за договором комерційної концесії; 6)не розголошувати секрети виробництва правоволодільця, іншу одержану від нього конфіденційну інформацію.	Article 1121 of the Civil Code of Ukraine: 1. Taking into account the nature and peculiarities of the activity carried out by the user under the commercial concession agreement, the user is obliged to: 1) use the trademark and other designations of the right holder in the manner specified in the contract; 2) ensure compliance of the quality of goods (works, services) produced (performed, provided) in accordance with the commercial concession agreement, the quality of similar goods (works, services) produced (performed, provided) by the right holder; 3) follow the instructions and guidelines of the right holder, aimed at ensuring compliance of the nature, methods and conditions of use of the set of granted rights to the use of these rights by the right holder; 4) provide buyers (customers) with additional services that they could count on when buying (ordering) goods (works, services) directly from the right holder; 5)to inform buyers (customers) in the most obvious way for them about their use of the trademark and other designations of the right holder under the commercial concession agreement; 6) not to disclose the secrets of the production of the right holder, other confidential information received from him.
Стаття 161 Кримінального кодексу України: Умисні дії, спрямовані на розпалювання національної, расової чи релігійної ворожнечі та ненависті, на приниження національної честі та гідності, або образа почуттів громадян у зв'язку з їхніми релігійними переконаннями, а також пряме чи непряме обмеження прав або встановлення прямих чи непрямих привілеїв громадян за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, інвалідності, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками,	Article 161 of the Criminal Code of Ukraine: Intentional actions aimed at inciting national, racial or religious hatred and hatred, degrading national honour and dignity, or insulting the feelings of citizens in connection with their religious beliefs, as well as directly or indirectly restricting the rights or establishing direct or indirect privileges of citizens for characteristics of race, skin colour, political, religious and other beliefs, gender, disability, ethnic and social origin, property status, place of residence, language or other characteristics, shall be punishable by a fine of two hundred to five hundred non-taxable minimum

караються штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.	incomes or restriction of liberty for up to five years, with deprivation of the right to hold certain positions or engage in certain activities for up to three years or without such.
Стаття 301 Кримінального кодексу України: 1. Ввезення в Україну творів, зображень або інших предметів порнографічного характеру з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою, або їх збут чи розповсюдження, а також примушування до участі в їх створенні, караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.	Article 301 of the Criminal Code of Ukraine: 1. Transporting works, pictures or other pornographic objects to Ukraine with the aim of marketing or distribution, or production, safe keeping, transferring or other transportation of such objects with the same aim, or their marketing or distribution, as well as forcing to create such kind of objects, are subjected to the following punishment: from 50 to 100 minimum income not exposed to tax or arrest up to 6 months, or imprisonment up to 3 years.
Частина 4 статті 9 Закону України «Про електронну комерцію»: Постачальник послуг проміжного характеру в інформаційній сфері не є стороною електронного правочину, предметом якого виступають товари, роботи або послуги, інші ніж послуги проміжного характеру в інформаційній сфері (реєстрація доменних імен або IP-адрес, присвоєння інших мережевих ідентифікаторів, фіксація часу відправлення/надходження електронного повідомлення, надання доступу до мережі Інтернет та інших інформаційно-телекомунікаційних систем тощо), і не несе відповідальності за зміст переданої чи отриманої інформації та за шкоду, завдану внаслідок використання результатів таких послуг, за умови, що він не є ініціатором передачі такої інформації, не обирає її одержувача та не може змінити її зміст. Постачальник послуг проміжного характеру в інформаційній сфері, що надає послуги проміжного (тимчасового) зберігання інформації, наданої одержувачем послуги, з єдиною метою - покращити подальшу передачу	Part 4 of the Article 9 of the Law of Ukraine 'On Electronic Commerce': The intermediary service provider in the information society is not a party to an electronic transaction, subject of which are products, works or services other than an intermediary service in the information society (domain name or IP address registration, assignment of other network IDs, fixation of sending/receiving time of e-mails, providing access to the Internet and other information and telecommunication systems, etc.), and is not responsible for the content of the information transmitted or received and for damages, resulted from the use of such services, provided that he does not initiate the transmission of such information, does not choose its recipient and cannot change its content. The intermediary service provider (caching) is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service at their request and for damages, resulted from the use of such services, provided that: one does not modify the

інформації іншим одержувачам послуги на їхню вимогу, не несе відповідальності за автоматичне, тимчасове та проміжне зберігання інформації і за шкоду, завдану внаслідок використання результатів таких послуг, за умови що він не змінює зміст інформації, виконує умови доступу до інформації, включаючи законодавчі вимоги доступу до інформації про власника мережевого ресурсу, виконує правила оновлення інформації у спосіб, який визнаний і використовується у промисловості, не перешкоджає законному використанню технологій, які визнані та використовуються у промисловості, при отриманні даних про використання інформації вдається до швидких дій з метою унеможливлення доступу до інформації, яку він зберігав, після того як йому стало відомо, що інформація в первинному джерелі передачі була видалена з мережі або доступ до неї унеможливлено, або є рішення суду про видалення чи унеможливлення доступу. Постачальник послуг проміжного характеру в інформаційній сфері, що надає послуги постійного зберігання інформації на запит одержувача послуг хостингу, не несе відповідальності за зміст переданої чи отриманої інформації, яка зберігається на запит отримувача послуг, та за шкоду, завдану внаслідок використання результатів таких послуг, за умови що у нього відсутні відомості про незаконну діяльність або факти чи обставини, які вказують на те, що діяльність має ознаки незаконної, або стосовно вимог про відшкодування збитків від такої незаконної діяльності, та постачальник після отримання таких відомостей вдається до швидких дій з метою усунення можливості доступу чи припинення доступу до інформації, у тому числі відповідно до вимог законодавства про авторське право і суміжні права.	information; complies with conditions on access to the information including legal requirements for access to information about the owner of the network resource; complies with rules regarding the updating of the information, specified in a manner recognised and used by industry; it does not interfere with the lawful use of technology, recognised and used by industry; it acts expeditiously to remove or to disable access to the information that was stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement. The intermediary service provider in the information society, that provides the services of permanent information caching at the request of a recipient of the hosting service, is not liable for the information stored at the request of a recipient of the service and for damages, results from the use of such services, provided that: one does not have actual knowledge of illegal activity or of facts or circumstances from which the illegal activity or information is apparent or regarding claims for damages and the provider; upon obtaining such knowledge acts expeditiously to remove or to disable access to the information, including the actions under the legislation on copyright law and related rights.
Стаття 1 Закону України «Про звернення громадян»: Громадяни України мають право звернутися до органів державної влади, місцевого самоврядування, об'єднань	Article 1 of the Law of Ukraine 'On citizens' appeals': Citizens of Ukraine have the right to apply to state bodies, local self-government, associations of citizens, enterprises,

громадян, підприємств, установ, організацій незалежно від форм власності, засобів масової інформації, посадових осіб відповідно до їх функціональних обов'язків із зауваженнями, скаргами та пропозиціями, що стосуються їх статутної діяльності, заявою або клопотанням щодо реалізації своїх соціально-економічних, політичних та особистих прав і законних інтересів та скаргою про їх порушення.	institutions, organisations regardless of ownership, mass media, officials according to their functional responsibilities with comments, complaints and proposals concerning their statutory activities, a statement or petition for the exercise of their socio-economic, political and personal rights and legitimate interests, and a complaint about their violation.
Пункт 18 частини 1 та частина 2 статті 39 Закону України «Про телекомунікації» : 1.Оператори телекомунікацій зобов'язані: 18) на підставі рішення суду обмежувати доступ своїх абонентів до ресурсів, через які здійснюється розповсюдження дитячої порнографії; 2. Усі пункти частини першої цієї статті, крім пунктів 1, 2, 10, 11, 12, 15, 17, 18^{-1}, поширюються також на провайдерів телекомунікацій. Оператори, провайдери телекомунікацій зберігають та надають інформацію про з'єднання свого абонента у порядку, встановленому законом.	Paragraph 18 of the part 1 and part 2 of the Article 39 of the Law of Ukraine 'On Telecommunications': 1.Telecommunication operators are obliged to: 18) on the basis of a court decision to restrict the access of its subscribers to the resources through which the distribution of child pornography is carried out; 2. All paragraphs of part one of this article, except for paragraphs 1, 2, 10, 11, 12, 15, 17, 18-1, shall also apply to telecommunications providers. Operators, telecommunications providers store and provide information about the connection of their subscriber in the manner prescribed by law.
Частина 4 статті 40 Закону України «Про телекомунікації» : 4. Оператори, провайдери телекомунікацій не несуть відповідальності за зміст інформації, що передається їх мережами.	Part 4 of the Article 40 of the Law of Ukraine 'On Telecommunications': 4.Operators, telecommunications providers are not responsible for the content of information transmitted by their networks.
Пункти 6-8 частини 1 статті 18 Закону України «Про правовий режим надзвичайного стану»: У разі введення надзвичайного стану з підстав, зазначених у пунктах 2-7 частини другої статті 4 цього Закону, додатково можуть здійснюватися такі заходи: 6) заборона виготовлення і розповсюдження інформаційних матеріалів, що можуть дестабілізувати обстановку; 7) регулювання роботи цивільних теле- та радіоцентрів, заборона роботи аматорських радіопередавальних засобів та радіовипромінювальних пристроїв особистого і колективного користування;	Paragraphs 6-8 of the part 1 of the Article 18 of the Law of Ukraine 'On the Legal Regime of the State of Emergency': In the event of a state of emergency on the grounds specified in paragraphs 2-7 of the second part of Article 4 of this Law, the following measures may be additionally carried out: 6) a ban on the production and dissemination of information materials that may destabilise the situation; 7) regulation of the work of civilian TV and radio centers, ban on the operation of amateur radio transmitters and radio emitting devices for personal and collective use;

8) особливі правила користування зв'язком та передачі інформації через комп'ютерні мережі;	8) special rules for the use of communication and transmission of information via computer networks;
Пункт 18 частини 1 статті 8 Закону України «Про правовий режим воєнного стану»: 1. В Україні або в окремих її місцевостях, де введено воєнний стан, військове командування разом із військовими адміністраціями (у разі їх утворення) можуть самостійно або із залученням органів виконавчої влади, Ради міністрів Автономної Республіки Крим, органів місцевого самоврядування запроваджувати та здійснювати в межах тимчасових обмежень конституційних прав і свобод людини і громадянина, а також прав і законних інтересів юридичних осіб, передбачених указом Президента України про введення воєнного стану, такі заходи правового режиму воєнного стану: 18) встановлювати порядок використання фонду захисних споруд цивільного захисту;	Paragraph 18 of part 1 of the Article 8 of the Law of Ukraine 'On the Legal regime of Martial State': 1. In Ukraine or in certain localities where martial law has been imposed, the military command together with military administrations (in case of their formation) may independently or with the involvement of executive bodies, the Council of Ministers of the Autonomous Republic of Crimea, local self-government bodies introduce and implement temporary restrictions on the constitutional rights and freedoms of man and citizen, as well as the rights and legitimate interests of legal entities provided by the decree of the President of Ukraine on the imposition of martial law, the following measures of the legal regime of martial law: 18) establish the procedure for using the fund of protective structures of civil protection;
Частина 1 статті 2 Закону України «Про захист суспільної моралі»: Виробництво та обіг у будь-якій формі продукції порнографічного характеру в Україні забороняються. Критерії віднесення продукції до такої, що має порнографічний характер, встановлюються центральним органом виконавчої влади, що забезпечує формування державної політики у сфері культури.	Part 1 of the Article 2 of the Law of Ukraine 'On the Protection of Public Morale': Production and circulation in any form of pornographic products in Ukraine is prohibited. Criteria for classifying products as pornographic are established by the central executive body, which ensures the formation of state policy in the field of culture.
Стаття 3 Закону України «Про звернення громадян»: Скарга - звернення з вимогою про поновлення прав і захист законних інтересів громадян, порушених діями (бездіяльністю), рішеннями державних органів, органів місцевого самоврядування, підприємств, установ, організацій, об'єднань громадян, посадових осіб.	Article 3 of the Law of Ukraine 'On citizens' appeals': Complaint - appeal with the request for restoration of rights and protection of the legitimate interests of citizens, violated by actions (inaction), decisions of state bodies, bodies of local self-government, enterprises, institutions, organisations, associations of citizens, officials.
Стаття 5 Закону України «Про інформацію»: 1. Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації,	Article 5 of the Law of Ukraine 'On Information': 1. Everyone has the right to information, which provides free receipt, use, dissemination, storage and protection of information necessary for the exercise of

необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.	their rights, freedoms and legitimate interests. The exercise of the right to information must not violate public, political, economic, social, spiritual, environmental and other rights, freedoms and legitimate interests of other citizens, the rights and interests of legal entities.
Стаття 11 Закону України «Про інформацію»: 1. Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.	Article 11 of the Law of Ukraine 'On Information': 1.Information about a natural person (personal data) - information or a set of information about a natural person who is identified or can be specifically identified.
Стаття 20 Закону України «Про інформацію»: 1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. 2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.	Article 20 of the Law of Ukraine 'On Information': 1. On the ground of access order information is divided into public one and information with a restricted access. 2. Any kind of information is public, except one that is legally referred as information with a restricted access.
Стаття 21 Закону України «Про інформацію»: 1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. 2. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом».	Article 21 of the Law of Ukraine 'On Information': 1. Restricted information is confidential, secret and on-duty information. 2. Information about an individual is confidential, as well as information access to which is restricted to an individual or a legal entity, except for the authorities. Confidential information may be disseminated at the request (consent) of the correspondent person in the manner prescribed by him or her, in accordance with the conditions stipulated by him, as well as in other cases stipulated by law.
Стаття 24 Закону України «Про інформацію»: Забороняється цензура - будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання в будь-якій іншій формі тиражуванню або поширенню інформації.» «Забороняються втручання у професійну діяльність журналістів, контроль за змістом поширюваної інформації,	Article 24 of the Law of Ukraine 'On Information': Censorship is prohibited - any requirement directed in particular to a journalist, the media, its founder (co-founder), the publisher, the manager, the distributor, to coordinate information before its dissemination or prohibition or interference with any other form of duplication or distribution of information. It is prohibited to interfere with the professional activities of journalists, to control the content of distributing information, in particular for the purpose of

зокрема з метою поширення чи непоширення певної інформації, замовчування суспільно необхідної інформації, накладення заборони на висвітлення окремих тем, показ окремих осіб або поширення інформації про них, заборони критикувати суб'єктивладних повноважень.	disseminating or not disseminating of certain information, concealing publicly required information, prohibiting the coverage of particular topics, the display of individuals or dissemination of information about them, prohibitions on criticising the authorities.
Стаття 28 Закону України «Про інформацію»: 1. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.	Article 28 of the Law of Ukraine 'On Information': 1. Information may not be used to call for the overthrow of the constitutional order, violation of the territorial integrity of Ukraine, propaganda of war, violence, cruelty, incitement of interethnic, racial, religious hatred, terrorist acts, encroachment on human rights and freedoms.
Стаття 29 Закону України «Про інформацію»: 1. Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. 2. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.	Article 29 of the Law of Ukraine 'On Information': 1. Information with a restricted access can be distributed if it is of a high social value, namely is a subject of social interest, and the citizens' right to information prevails a potential damage from the disclosure. 2. A subject of social interest is considered to be information that indicates a threat to national sovereignty, territorial integrity of Ukraine; ensures execution of constitutional rights , freedoms and obligations; proclaims a possibility of human rights violation, delusion of citizens, harmful ecological and other detrimental results of action (inaction) of individuals and juristic persons, etc.
Стаття 30 Закону України «Про інформацію»: Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень. Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол,	Article 30 of the Law of Ukraine 'On information': Nobody shall be charged for expression of evaluation judgements. Evaluation judgements, excepting slander, are judgements which do not comprise factual evidence, criticism, evaluation of actions and statements that cannot be interpreted as containing factual data, in particular in view of the nature of the use of linguistic and stylistic means (use hyperbole, allegory, satire). Evaluation judgements are

алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.	not subject to refutation and proving their veracity.
Частина 7 статті 52-1 Закону України «Про авторське право і суміжні права»: 7. Заявник має право звернутися безпосередньо до постачальника послуг хостингу, який надає послуги і (або) ресурси для розміщення відповідного веб-сайту, із заявою про припинення порушення, допущеного власником веб-сайту, в таких випадках: а) власник веб-сайту у встановлені цією статтею строки не вчинив або вчинив не в повному обсязі дії, передбачені частиною третьою або п'ятою цієї статті, або якщо власник веб-сайту, який не є власником веб-сторінки, не вчинив дій або вчинив не в повному обсязі дії, передбачені частиною шостою цієї статті; б) на веб-сайті та в публічних базах даних записів про доменні імена (WHOIS) відсутні відомості про власника веб-сайту в обсязі, що дає змогу звернутися до нього із заявою про припинення порушення, передбаченою частиною другою цієї статті. У разі якщо впродовж 24 годин з моменту направлення власнику веб-сайту копії заяви про припинення порушення власник веб-сайту не вчинив дій, передбачених абзацом восьмим цієї частини, постачальник послуг хостингу самостійно унеможливлює доступ до електронної (цифрової) інформації, зазначеної у заяві про припинення порушення, допущеного власником веб-сайту. Про вжиті заходи постачальник послуг хостингу повідомляє заявника та власника веб-сайту впродовж 48 годин з моменту отримання постачальником послуг хостингу заяви про припинення порушення, допущеного власником веб-сайту.	Part 7 of the Article 52-1 of the Law of Ukraine 'On copyright law and related rights': 7. Applicant has the right to apply directly to the hosting provider who provides services and\or resources for hosting a relevant website, with a request to terminate the violation, in the following cases: a) the owner of website did not take any actions or did not fully take actions, provided for under p.3 or p.5 of this article, or if the owner of website, who is not the owner of the webpage, did not take any actions or did not fully take actions, provided for under p.6 of this article; b) there is no information about the website owner on the website and in the public databases on domain names (WHOIS) to the extent which allows to submit a request on the termination of violation to him, envisaged by p.2 of this article. In case if the owner of website did not take actions, provided for by p.8 of this article, during 24 hours after the copy of the request for termination of violation was sent to him, the hosting provider shall deny access to electronic (digital) information, mentioned in the request for termination of violation, admitted by the website owner, on his own. The hosting provider notifies the applicant and website owner about the measures taken during 48 hours from the moment the hosting provider received the request for termination of violation, admitted by website owner.
Частина 2 статті 52-2 Закону України «Про авторське право і суміжні права»: 2. Постачальник послуг хостингу не несе перед замовником таких послуг відповідальності за наслідки вжиття заходів, передбачених статтею 52-1 цього	Part 2 of the Article 52-2 of the Law of Ukraine 'On copyright law and related rights': 2. The hosting service provider shall not be liable to the customer of such services for the consequences of taking the measures provided for in Article 52-1 of this Law,

Закону, за умови виконання вимог частини першої цієї статті. Постачальник послуг хостингу не несе відповідальності за порушення авторського права і (або) суміжних прав, за умови виконання вимог статті 52-1 цього Закону.	provided that the requirements of part one of this Article are met. The hosting service provider shall not be liable for infringement of copyright and (or) related rights, provided that the requirements of Article 52-1 of this Law are met.
Частина 3 статті 5 Закону України «Про захист персональних даних»: 3. Персональні дані, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, оформленій за формою, визначеною відповідно до Закону України "Про запобігання корупції", не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України 'Про запобігання корупції'.	Part 3 of the Article 5 of the Law of Ukraine 'On Protection of Personal Data': 3. Personal data specified in the declaration of a person authorised to perform the functions of state or local self-government, drawn up in the form specified in accordance with the Law of Ukraine 'On Prevention of Corruption', do not belong to restricted information, except for information specified by the Law of Ukraine 'On Prevention of Corruption'.
Пункти 5, 6, 11 частини 2 статті 8 Закону України «Про захист персональних даних»: 2. Суб'єкт персональних даних має право: 5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних; 6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними; 11) відкликати згоду на обробку персональних даних;	Subsections 5, 6, 11 of section 2 of the Article 3 of the Law of Ukraine 'On Protection of Personal Data': 2. An identifiable person has the right to: 5) make a motivated request to a controller to prohibit the processing of his/her personal data; 6) make a motivated request to amend or destroy his/her personal data by a controller or processor if such data is processed illegally or is unreliable; 11) revoke his/her consent to personal data processing.
Стаття 15 Закону України «Про захист персональних даних»: 1.Персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону. 2.Персональні дані підлягають видаленню або знищенню у разі: 1)закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; 2)припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;	Article 15 of Law of Ukraine 'On Protection of Personal Data': 1. Personal data is deleted or destroyed in the manner prescribed by law. 2. Personal data is to be deleted or destroyed in the event: 1) the term of data storage, determined by the consent of an identifiable person or the Privacy Law has expired; 2) legal relations between an identifiable person and a data controller or processor have seized to exist unless otherwise provided by law;

3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних. 3. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку. 4. Персональні дані, зібрані під час виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом, видаляються або знищуються відповідно до вимог закону.	3) the Ukrainian Parliament Commissioner for Human Rights has issued a relevant instruction to do so; 4) a court decision, ruling to remove or destroy personal data has entered into legal force. 3. Personal data, collected in a way that violated the requirements of this Law shall be deleted or destroyed in a manner prescribed by law. 4. Personal data, collected during the course of intelligence-led policing, counterintelligence or terrorism prevention, shall be deleted or destroyed in a manner prescribed by law.
Стаття 2 Закону України «Про друковані засоби масової інформації (пресу) в Україні» : Забороняється створення та фінансування державних органів, установ, організацій або посад для цензури масової інформації. Не допускається вимога попереднього погодження повідомлень і матеріалів, які поширюються друкованими засобами масової інформації, а також заборона поширення повідомлень і матеріалів з боку посадових осіб державних органів, підприємств, установ, організацій або об'єднань громадян».	Article 2 of the Law of Ukraine 'On the Print Media (Press) in Ukraine': It is forbidden to create and finance state bodies, institutions, organisations or positions for censorship of the media. The requirement for prior approval of messages and materials disseminated by print media, as well as the prohibition of dissemination of messages and materials by officials of state bodies, enterprises, institutions, organisations or associations of citizens should not be allowed.
Частина 7 статті 4 Закону України «Про телебачення і радіомовлення»: 7. Держава всіма можливими законними засобами не допускає в інформаційних та інших телерадіопрограмах систематичного цілеспрямованого безпідставного загострення уваги на війні, насильстві і жорстокості, розпалюванні расової, національної та релігійної ворожнечі або позитивного їх подання (трактування), а також забезпечує ідеологічний і політичний плюралізм у сфері аудіовізуальних засобів масової інформації.	Part 7 of the Article 4 of the Law of Ukraine 'On television and Radio Broadcasting': 7. The state by all possible legal means does not allow in information and other TV and radio programs systematic purposeful unreasonable aggravation of attention on war, violence and cruelty, incitement of racial, national and religious enmity or their positive representation (interpretation), and also provides ideological and political audiovisual media.
Стаття 5 Закону України «Про телебачення і радіомовлення»:	Article 5 of the Law of Ukraine 'On television and Radio Broadcasting':

Цензура інформаційної діяльності телерадіоорганізації забороняється. Телерадіоорганізація є незалежною у визначенні змісту програм та передач. Не вмотивоване законодавством України втручання органів державної влади чи органів місцевого самоврядування, громадських чи релігійних об'єднань, їх посадових осіб чи працівників, а також власників у сферу професійної діяльності телерадіоорганізацій не допускається.	Censorship of information activities of a broadcasting organisation is prohibited. The broadcasting organisation is independent in determining the content of programs and broadcasts. Interference by state or local governments, public or religious associations, their officials or employees, as well as owners in the sphere of professional broadcasting organisations is not allowed by the legislation of Ukraine.
Частина 2 статті 6 Закону України «Про телебачення і радіомовлення»: 2. Не допускається використання телерадіоорганізацій для: поширення відомостей, що становлять державну таємницю, або іншої інформації, яка охороняється законом; закликів до насильницької зміни конституційного ладу України; закликів до розв'язування агресивної війни або її пропаганди та/або розпалювання національної, расової чи релігійної ворожнечі та ненависті; необґрунтованого показу насильства; пропаганди винятковості, зверхності або неповноцінності осіб за ознаками їх релігійних переконань, ідеології, належності до тієї чи іншої нації або раси, фізичного або майнового стану, соціального походження; трансляції програм та передач, у яких телеглядачам та/або радіослухачам надаються послуги з ворожіння та гадання, а також платні послуги у сфері народної та/або нетрадиційної медицини; трансляції програм або їх відеосюжетів, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків, якщо вони мають змогу їх дивитися; трансляції телепередач, виготовлених після 1 серпня 1991 року, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що виправдовують чи визнають правомірною окупацію території України. Для цілей застосування цієї норми використовуються визначення та критерії,	Part 2 of the Article 6 of the Law of Ukraine 'On television and Radio Broadcasting': 2. The use of television and radio organisations for: dissemination of information constituting a state secret or other information protected by law; calls for a violent change of the constitutional order of Ukraine; calls for an aggressive war or its propaganda and / or incitement to national, racial or religious hatred and hatred; unreasonable display of violence; propaganda of exclusivity, superiority or inferiority of persons on the grounds of their religious beliefs, ideology, belonging to a particular nation or race, physical or property status, social origin; broadcasting of programs and programs in which TV and / or radio listeners are provided with divination and divination services, as well as paid services in the field of folk and / or alternative medicine; broadcast programs or their videos that may harm the physical, mental or moral development of children and adolescents if they are able to watch them; broadcasts of television programs made after August 1, 1991, containing popularisation or propaganda of the bodies of the aggressor state and their individual actions that justify or recognise the lawful occupation of the territory of Ukraine. For the purposes of application of this norm the definitions and criteria established by the Law of Ukraine 'On Cinematography' are used; broadcasting of audiovisual works (films, TV programs, except for information and

встановлені Законом України "Про кінематографію"; трансляції аудіовізуальних творів (фільмів, телепередач, крім інформаційних та інформаційно-аналітичних телепередач), одним із учасників яких є особа, внесена до Переліку осіб, які створюють загрозу національній безпеці, оприлюдненого на веб-сайті центрального органу виконавчої влади, що забезпечує формування державної політики у сферах культури та мистецтв. При цьому учасником аудіовізуального твору вважається фізична особа, яка брала участь у його створенні під власним ім'ям (псевдонімом) або як виконавець будь-якої ролі, виконавець музичного твору, що використовується в аудіовізуальному творі, автор сценарію та/або текстів чи діалогів, режисер-постановник, продюсер; розповсюдження і реклами порнографічних матеріалів та предметів; пропаганди наркотичних засобів, психотропних речовин з будь-якою метою їх застосування; поширення інформації, яка порушує законні права та інтереси фізичних і юридичних осіб, посягає на честь і гідність особи; здійснення інших вчинків, за якими наступає кримінальна відповідальність.	information-analytical TV programs), one of the participants of which is a person included in the List of persons who pose a threat to national security, published on the website of the central executive body in the fields of culture and arts. A participant in an audiovisual work is a natural person who participated in its creation under his own name (pseudonym) or as a performer of any role, performer of a musical work used in an audiovisual work, author of a script and / or texts or dialogues, director, producer; distribution and advertising of pornographic materials and objects; propaganda of narcotic drugs, psychotropic substances for any purpose of their use; dissemination of information that violates the legal rights and interests of individuals and legal entities, infringes on the honour and dignity of the person; committing other acts for which criminal liability occurs.
Стаття 72 Закону України «Про телебачення і радіомовлення»: 1. Санкції за порушення законодавства про телебачення і радіомовлення застосовуються за рішенням суду або, у встановлених цим Законом випадках, за рішенням Національної ради. 2.Національна рада застосовує санкції до телерадіоорганізацій у разі порушення ними вимог цього Закону та/або умов ліцензії. 3.Національна рада застосовує санкції до провайдерів програмної послуги у разі порушення ними вимог цього Закону та/або умов ліцензії. 4.У разі порушення законодавства про телебачення і радіомовлення іншими юридичними або фізичними особами	Article 72 of the Law of Ukraine 'On television and Radio Broadcasting': 1. Sanctions for violation of the legislation on television and radio broadcasting shall be applied by a court decision or, in cases established by this Law, by a decision of the National Council. 2. The National Council shall apply sanctions to television and radio organisations in case they violate the requirements of this Law and / or the terms of the license. 3. The National Council shall apply sanctions to software service providers in case they violate the requirements of this Law and / or the terms of the license. 4. In case of violation of the legislation on television and radio broadcasting by other

Національна рада звертається до суду або до інших органів державної влади для усунення цих порушень у визначеному законодавством порядку. 5. Національна рада приймає рішення про застосування санкцій на підставі наданих документальних свідчень, актів перевірки чи подання визначених цим Законом органів державної влади. 6.Національна рада може застосовувати до телерадіоорганізацій та провайдерів програмної послуги такі санкції: оголошення попередження; стягнення штрафу; анулювання ліцензії на підставі рішення суду за позовом Національної ради. 7.Рішення про оголошення попередження приймається у разі першого порушення законодавства чи умов ліцензії телерадіоорганізацією або першого порушення законодавства провайдером програмної послуги. 8. Національна рада може прийняти рішення про стягнення штрафу в зазначених у цій частині розмірах, незалежно від застосування до порушника санкцій у вигляді попередження, виключно в разі вчинення таких порушень: телерадіоорганізаціями - 25 відсотків розміру ліцензійного збору за: заклики до насильницької зміни конституційного ладу України; заклики до розв'язування агресивної війни або її пропаганди та/або розпалювання національної, расової чи релігійної ворожнечі та ненависті; пропаганду винятковості, зверхності або неповноцінності осіб за ознаками їх релігійних переконань, ідеології, належності до тієї чи іншої нації або раси, фізичного або майнового стану, соціального походження; провайдерами програмної послуги - 25 відсотків розміру ліцензійного збору за: ретрансляцію програм та передач, щодо яких Національною радою прийнято рішення, що їх зміст не відповідає вимогам законодавства України відповідно до статті 42 цього Закону;	legal or natural persons, the National Council shall apply to a court or other public authorities to eliminate these violations in the manner prescribed by law. 5. The National Council shall make a decision on the application of sanctions on the basis of the provided documentary evidence, acts of inspection or submission of public authorities specified by this Law. 6. The National Council may apply the following sanctions to broadcasters and program service providers: warning announcement; collection of a fine; revocation of the license on the basis of a court decision at the suit of the National Council. 7. The decision to announce a warning is made in case of the first violation of the law or the terms of the license by the television and radio organisation or the first violation of the law by the software service provider. 8. The National Council may decide to impose a fine in the amounts specified in this part, regardless of the application of sanctions to the violator in the form of a warning, only in the case of the following violations: TV and radio organisations - 25 percent of the license fee for: calls for a violent change of the constitutional order of Ukraine; calls for an aggressive war or its propaganda and / or incitement to national, racial or religious hatred and hatred; propaganda of exclusivity, superiority or inferiority of persons on the grounds of their religious beliefs, ideology, belonging to a particular nation or race, physical or property status, social origin; software service providers - 25 percent of the license fee for: retransmission of programs and programs in respect of which the National Council has decided that their content does not meet the requirements of the legislation of Ukraine in accordance with Article 42 of this Law; retransmission of programs and programs prohibited and / or restricted by the court. If calls for a violent change of the constitutional order of Ukraine, the

ретрансляцію програм та передач, заборонених та/або обмежених судом. У разі якщо заклики до насильницької зміни конституційного ладу України, розв'язування агресивної війни або її пропаганди та/або розпалювання національної, расової чи релігійної ворожнечі та ненависті, пропаганди винятковості, зверхності або неповноцінності осіб за ознаками їх релігійних переконань, ідеології, належності до тієї чи іншої нації або раси, фізичного або майнового стану, соціального походження транслювалися, поширювалися, розповсюджувалися без попереднього запису та містилися у виступах, репліках особи, яка не є працівником телерадіоорганізації, телерадіоорганізація не несе відповідальності за ці порушення, крім випадків, коли працівниками телерадіоорганізації не було вжито заходів щодо припинення правопорушення у прямому ефірі. 9. Рішення про стягнення штрафу приймається Національною радою, якщо після оголошення попередження ліцензіат не усунув порушення в установлені Національною радою строки, у разі вчинення таких порушень: телерадіоорганізаціями - 10 відсотків розміру ліцензійного збору за: трансляцію програм та передач, у яких телеглядачам та/або радіослухачам надаються послуги з ворожіння та гадання, а також платні послуги у сфері народної та/або нетрадиційної медицини; трансляцію програм та передач або їх відеосюжетів, що можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків, якщо програма, передача або відеосюжет демонструвалися з порушенням часу демонстрування або не мали візуальних позначок з індексом кіновідеопродукції залежно від аудиторії, на яку вони розраховані, у порядку, передбаченому цим Законом;	outbreak of aggressive war or its propaganda and / or incitement to national, racial or religious enmity and hatred, propaganda of exclusivity, superiority or inferiority of persons on the grounds of their religious beliefs, ideology, belonging to that or other nation or race, physical or property status, social origin were broadcast, disseminated, distributed without prior recording and contained in speeches, remarks of a person who is not an employee of the broadcaster, the broadcaster is not responsible for these violations, except when employees of non-broadcasters measures were taken to stop the offense live. 9. The decision to impose a fine is made by the National Council, if after the announcement of the warning the licensee has not eliminated the violation within the time limits set by the National Council, in case of such violations: TV and radio organisations - 10 percent of the license fee for: broadcasting of programs and programs in which TV and / or radio listeners are provided with divination and divination services, as well as paid services in the field of folk and / or alternative medicine; broadcast programs and programs or their videos that may harm the physical, mental or moral development of children and adolescents, if the program, program or video was shown in violation of the show time or did not have visual markings with the index of film and video production, depending on the audience for which they are intended, in the manner prescribed by this Law; broadcasting of television programs made after August 1, 1991, which contain popularisation or propaganda of the bodies of the aggressor state and their individual actions that justify or recognise the lawful occupation of the territory of Ukraine. For the purposes of application of this norm the definitions and criteria established by the Law of Ukraine 'On cinematography' are used; broadcasting of audiovisual works, TV programs, except for information and

трансляцію телепередач, виготовлених після 1 серпня 1991 року, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що виправдовують чи визнають правомірною окупацію території України. Для цілей застосування цієї норми використовуються визначення та критерії, встановлені Законом України "Про кінематографію"; трансляцію аудіовізуальних творів, телепередач, крім інформаційних та інформаційно-аналітичних, одним з учасників яких є особа, внесена до Переліку осіб, які створюють загрозу національній безпеці, затвердженого центральним органом виконавчої влади, що забезпечує формування державної політики у сферах культури та мистецтв, та оприлюдненого на офіційному веб-сайті цього органу; розповсюдження і рекламу порнографічних матеріалів та предметів; пропаганду наркотичних засобів, психотропних речовин з будь-якою метою їх застосування; 5 відсотків розміру ліцензійного збору за порушення умов ліцензії, визначених ліцензією на мовлення та додатками до неї, та/або ліцензійних умов (крім вимог до організаційно-технічних, фінансових та інвестиційних зобов'язань ліцензіата) у частині програмної концепції; провайдерами програмної послуги - 10 відсотків розміру ліцензійного збору за незабезпечення абонентам можливості перегляду програм універсальної програмної послуги; 5 відсотків розміру ліцензійного збору за порушення умов ліцензії, визначених ліцензією та додатками до неї, та/або ліцензійних умов. 10.Штраф не може накладатися, якщо з часу порушення законодавства, за яке він може бути застосований, минуло більше одного календарного року. 11.Розрахунок розмірів штрафів здійснюється відповідно до нарахованого розміру ліцензійного збору ліцензіату за видачу ліцензії, не враховуючи умов (зменшення/збільшення), що діє на	information-analytical, one of the participants of which is a person included in the List of persons posing a threat to national security, approved by the central executive body, which ensures the formation of state policy in culture and arts, and published on the official website of this body; distribution and advertising of pornographic materials and objects; propaganda of narcotic drugs, psychotropic substances for any purpose of their use; 5 percent of the license fee for violation of the license conditions specified in the broadcasting license and its annexes, and / or license conditions (except for the requirements of organisational, technical, financial and investment obligations of the licensee) in parts of the program concept; software service providers - 10 percent of the license fee for failure to provide subscribers with the opportunity to view programs of the universal software service; 5 percent of the license fee for violation of the license conditions specified in the license and its annexes, and / or license conditions. 10. A fine may not be imposed if more than one calendar year has elapsed since the violation of the legislation for which it may be applied. 11. The calculation of fines is carried out in accordance with the accrued license fee of the licensee for the issuance of a license, not taking into account the conditions (reduction / increase) in force at the time of the National Council decision to impose a fine. For non-compliance with the requirements provided for in parts one-three and five of Article 9 of this Law, a television and radio broadcasting organisation shall pay a fine of 5 percent of the total license fee issued in accordance with the broadcasting license. For non-compliance with the requirements established by Article 10 of this Law, the broadcasting broadcaster shall pay a fine of 5 percent of the total amount of the license fee issued in accordance with the broadcasting license.

момент прийняття Національною радою рішення про накладення штрафу. За невиконання вимог, передбачених частинами першою- третьою та п'ятою статті 9 цього Закону, телерадіоорганізація, що здійснює радіомовлення, сплачує штраф у розмірі 5 відсотків загальної суми ліцензійного збору ліцензії, виданої відповідно до ліцензії на мовлення. За невиконання вимог, встановлених статтею 10 цього Закону, телерадіоорганізація, що здійснює мовлення, сплачує штраф у розмірі 5 відсотків загальної суми ліцензійного збору ліцензії, виданої відповідно до ліцензії на мовлення. За неподання або несвоєчасне подання інформації, передбаченої частиною другою статті 59 (для телерадіоорганізацій) або частиною дев'ятою статті 40 (для провайдерів програмної послуги) цього Закону, телерадіоорганізація або провайдер програмної послуги сплачує штраф у розмірі 5 відсотків загальної суми ліцензійного збору за всіма ліцензіями, власниками яких є порушник, відповідно до статті 31 цього Закону. У разі якщо ліцензіат має декілька ліцензій на мовлення з різними способами розповсюдження телерадіопрограм, з однаковою програмною концепцією мовлення, розмір штрафу встановлюється з найбільшого нарахованого розміру ліцензійного збору. У разі якщо один ліцензіат має декілька ліцензій з однаковими способами розповсюдження телерадіопрограм, з однаковою програмною концепцією мовлення на різних територіях мовлення, розмір штрафу встановлюється шляхом складання сум штрафів, що будуть нараховані за відповідні порушення. 12. Рішення про стягнення штрафу може бути оскаржене в судовому порядку. 13. Якщо порушення не були усунені після застосування санкції у вигляді стягнення штрафу, Національна рада звертається до суду з позовом про	For non-submission or late submission of information provided for in part two of Article 59 (for television and radio organisations) or part nine of Article 40 (for software service providers) of this Law, the television and radio organisation or program service provider shall pay a fine of 5 percent of the total license fee for all licenses , the owners of which are the violator, in accordance with Article 31 of this Law. If the licensee has several broadcasting licenses with different methods of distribution of television and radio programs, with the same program concept of broadcasting, the amount of the fine is set from the largest accrued license fee. If one licensee has several licenses with the same methods of distribution of television and radio programs, with the same program concept of broadcasting in different broadcasting territories, the amount of the fine is set by adding the amounts of fines that will be charged for the violations. 12. The decision to impose a fine may be appealed in court. 13. If the violations have not been remedied after the application of the sanction in the form of a fine, the National Council shall apply to the court for revocation of the broadcasting license or revocation of the license of the program service provider. A broadcaster or program service provider shall be deemed not to have been prosecuted in the form of a fine, if within one year from the date of the decision to impose a fine they have not repeatedly committed a violation under the same provision of this Law.

анулювання ліцензії на мовлення телерадіоорганізації або анулювання ліцензії провайдера програмної послуги. Телерадіоорганізація чи провайдер програмної послуги вважаються такими, що не притягалися до відповідальності у вигляді стягнення штрафу, якщо протягом одного року з дня прийняття рішення про стягнення штрафу вони повторно не вчиняли порушення, передбаченого таким самим положенням цього Закону.	
Стаття 15-1 Закону України «Про кінематографію»: В Україні забороняється розповсюдження і демонстрування фільмів, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що створюють позитивний образ працівників держави-агресора, працівників радянських органів державної безпеки, виправдовують чи визнають правомірною окупацію території України, а також забороняється трансляція (демонстрування шляхом показу каналами мовлення) фільмів, вироблених фізичними та юридичними особами держави-агресора. Передбачена частиною першою цієї статті заборона розповсюдження і демонстрування фільмів, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, поширюється на розповсюдження та демонстрування будь-яких фільмів незалежно від країни походження, вироблених після 1 серпня 1991 року. Заборона трансляції фільмів, вироблених фізичними та юридичними особами держави-агресора, які не містять популяризації або пропаганди органів держави-агресора та їхніх окремих дій, поширюється на фільми, вироблені та/або вперше оприлюднені (демонстровані) після 1 січня 2014 року. Фільм вважається таким, що містить популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що створює позитивний образ працівників держави-агресора, працівників радянських	Article 15-1 of the Law of Ukraine 'On Cinematography': Ukraine prohibits the distribution and showing of films that promote or promote the aggressor state and their individual actions that create a positive image of the aggressor state, Soviet security officers, justify or recognise the legitimate occupation of Ukraine, and broadcast (demonstration by showing through broadcast channels) films produced by individuals and legal entities of the aggressor state. The first part of this article prohibits the distribution and screening of films containing the promotion or promotion of the aggressor State's authorities and their individual actions, applies to the distribution and screening of any film, regardless of the country of origin, produced after 1 August 1991. The ban on broadcasting films produced by individuals and legal entities of the aggressor state, which do not contain the promotion or propaganda of the aggressor state's bodies and their individual actions, applies to films produced and / or first released (shown) after January 1, 2014. The film is considered to contain popularisation or propaganda of the aggressor state and their individual actions, which creates a positive image of the aggressor state, Soviet state security officers, justifies or recognises the lawful occupation of Ukraine, if it has at least one of these features. : among the positive heroes of the film are employees (including former or freelance) of the aggressor state, Soviet security agencies;

органів державної безпеки, виправдовує чи визнає правомірною окупацію території України, якщо в ньому наявна принаймні одна з таких ознак: серед позитивних героїв фільму є співробітники (у тому числі колишні або позаштатні) органів держави-агресора, радянських органів безпеки; сюжет фільму безпосередньо або опосередковано пов'язаний з діяльністю органів держави-агресора, радянських органів безпеки, і ця діяльність представлена у фільмі як позитивна; у сюжеті фільму безпосередньо або опосередковано заперечується або ставиться під сумнів територіальна цілісність України, виправдовується або подається в позитивному світлі окупація території України, акти агресії з боку інших держав, розв'язування війни, пропагується винятковість, зверхність або неповноцінність осіб за ознаками їх релігійних переконань, належності до певної нації або раси, статі, майнового стану, соціального походження. Центральний орган виконавчої влади, що реалізує державну політику в сфері кінематографії забезпечує реалізацію цього Закону шляхом прийняття рішення про віднесення фільмів до заборонених до розповсюдження і демонстрування на території України виключно на підставі ознак, визначених у статті 15-1 цього Закону. Державне посвідчення на право розповсюдження і демонстрування фільмів, передбачених частиною першою цієї статті, не видається. Розповсюдження та/або демонстрування фільмів, зазначених у частині першій цієї статті, тягне за собою застосування до суб'єктів господарювання, що здійснюють таке розповсюдження та/або демонстрування, адміністративно-господарських санкцій у формі накладення адміністративно-господарського штрафу в розмірі десяти мінімальних заробітних плат за кожен випадок такого розповсюдження або демонстрування, вчинений вперше, та у розмірі п'ятдесяти мінімальних	the plot of the film is directly or indirectly related to the activities of the aggressor state, the Soviet security services, and this activity is presented in the film as positive; the plot of the film directly or indirectly denies or questions the territorial integrity of Ukraine, justifies or presents in a positive light the occupation of Ukraine, acts of aggression by other states, the outbreak of war, promotes the exclusivity, superiority or inferiority of persons on the grounds of their religious beliefs, belonging to a particular nation or race, sex, property status, social origin. The central executive body implementing the state policy in the field of cinematography shall ensure the implementation of this Law by deciding to classify films as prohibited for distribution and showing on the territory of Ukraine solely on the basis of the features specified in Article 15-1 of this Law. The state certificate for the right to distribute and show films provided for in part one of this article shall not be issued. Distribution and / or showing of films referred to in part one of this Article shall entail the application to economic entities engaged in such distribution and / or showing of administrative and economic sanctions in the form of imposition of an administrative and economic fine in the amount of ten minimum wages. for each case of such distribution or demonstration committed for the first time, and in the amount of fifty minimum wages for each subsequent case of such distribution or demonstration. The decision to impose a fine provided for in part six of this article shall be made by the central executive body that implements the state policy in the field of cinematography. Reasons and justifications for determining the amount of the administrative and economic fine must be contained in the decision to impose a fine.

заробітних плат за кожен наступний випадок такого розповсюдження або демонстрування. Рішення про накладення штрафу, передбаченого частиною шостою цієї статті, приймає центральний орган виконавчої влади, що реалізує державну політику у сфері кінематографії. Мотиви та обґрунтування щодо визначення розміру адміністративно-господарського штрафу мають міститися в рішенні про накладення штрафу.	
Стаття 2 Закону України «Про інформаційні агентства»: Забороняється цензура інформації, поширюваної інформаційними агентствами.	Article 2 of the Law of Ukraine 'On news agencies': Censorship of information disseminated by news agencies is prohibited.
Стаття 1 Закону України «Про доступ до публічної інформації»: 1. Публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом. 2. Публічна інформація є відкритою, крім випадків, встановлених законом.	Article 1 of the Law of Ukraine 'On access to Public Information': 1. Public information is information reflected and documented by any means and on any media, which was received or created in the course of performance by subjects of power of the duties provided by the current legislation, or which is in possession of objects of power, other managers of public information, defined by this Law. 2. Public information is open, except in cases established by law.
Стаття 5 Закону України «Про доступ до публічної інформації»: 1. Доступ до інформації забезпечується шляхом: 1) систематичного та оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом; 2) надання інформації за запитами на інформацію.	Article 5 of the Law of Ukraine 'On access to Public Information': 1. Access to information is provided by: 1) systematic and prompt disclosure of information: in official printed publications; on official websites on the Internet; on the only state web portal of open data; on information stands; in any other way; 2) providing information on requests for information.

Стаття 6 Закону України «Про доступ до публічної інформації»: Інформацією з обмеженим доступом є: конфіденційна інформація, таємна інформація, службова інформація. Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог: 1)виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.	Article 6 of the Law of Ukraine 'On access to Public Information': Information with restricted access is: confidential information, classified information, official information. Restriction of access to information is carried out in accordance with the law in compliance with the totality of the following requirements: 1) solely in the interests of national security, territorial integrity or public order to prevent disturbance or crime, to protect the health of the population, to protect the reputation or rights of others, to prevent the disclosure of confidential information or to maintain the authority and impartiality of justice; 2) disclosure of information may cause significant harm to these interests; 3) the harm from the disclosure of such information outweighs the public interest in obtaining it.
Частини 3, 4 статті 10 Закону України «Про Раду національної безпеки і оборони України»: Прийняті рішення вводяться в дію указами Президента України. Рішення Ради національної безпеки і оборони України, введені в дію указами Президента України, є обов'язковими до виконання органами виконавчої влади.	Parts 3, 4 of the Article 10 of the Law of Ukraine 'On the National Security and Defence Council of Ukraine': The adopted decisions are put into effect by decrees of the President of Ukraine. Decisions of the National Security and Defence Council of Ukraine, enacted by decrees of the President of Ukraine, are binding on the executive branch.
Частина 1 статті 7 Закону України «Про доступ до публічної інформації»: 1.Конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 цього Закону.	Part 1 of the Article 7 of the Law of Ukraine 'On access to Public Information': 1.Confidential information - information to which access is restricted by a natural or legal person, except for subjects of power, and which may be disseminated in the manner prescribed by them at their request in accordance with the conditions provided by them. The information specified in parts one and two of Article 13 of this Law may not be classified as confidential.
Стаття 8 Закону України «Про доступ до публічної інформації»: 1. Таємна інформація - інформація, доступ до якої обмежується відповідно	Article 8 of the Law of Ukraine 'On access to Public Information': 1. Classified information - information to which access is restricted in accordance with

до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю. 2. Порядок доступу до таємної інформації регулюється цим Законом та спеціальними законами.	part two of Article 6 of this Law, the disclosure of which may harm the person, society and the state. Information that contains state, professional, banking secrets, pre-trial investigation secrets and other secrets provided by law is considered secret. 2. The procedure for access to classified information is regulated by this Law and special laws.
Частина 1 статті 21 Закону України «Про державну статистику» Первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов'язаною із збиранням та використанням адміністративних даних, є конфіденційною інформацією, яка охороняється Законом і використовується виключно для статистичних цілей у зведеному знеособленому вигляді.	Part 1 of the Article 21 of the Law of Ukraine 'On State Statistics': Primary data obtained by state statistics bodies from respondents during statistical observations, as well as administrative data on respondents obtained by state statistics bodies from bodies engaged in activities related to the collection and use of administrative data, are confidential information protected by law and is used exclusively for statistical purposes in a consolidated impersonal form.
Частина 1 статті 1 Закону України «Про санкції»: 1.З метою захисту національних інтересів, національної безпеки, суверенітету і територіальної цілісності України, протидії терористичній діяльності, а також запобігання порушенню, відновлення порушених прав, свобод та законних інтересів громадян України, суспільства та держави можуть застосовуватися спеціальні економічні та інші обмежувальні заходи (далі - санкції).	Part 1 of the Article 1 of the Law of Ukraine 'On Sanctions': 1. In order to protect the national interests, national security, sovereignty and territorial integrity of Ukraine, counter terrorist activity, as well as prevent violations, restore violated rights, freedoms and legitimate interests of citizens of Ukraine, society and the state, special economic and other restrictive measures may be applied. - sanctions).
Стаття 4 Закону України «Про санкції»: 1. Видами санкцій згідно з цим Законом є: 1) блокування активів - тимчасове обмеження права особи користуватися та розпоряджатися належним їй майном; 2) обмеження торговельних операцій; 3) обмеження, часткове чи повне припинення транзиту ресурсів, польотів та перевезень територією України; 4) запобігання виведенню капіталів за межі України;	Article 4 of the Law of Ukraine 'On Sanctions': 1. Types of sanctions under this Law are: 1) blocking of assets - temporary restriction of a person's right to use and dispose of property belonging to him; 2) restriction of trade operations; 3) restriction, partial or complete cessation of transit of resources, flights and transportation through the territory of Ukraine;

5) зупинення виконання економічних та фінансових зобов'язань; 6) анулювання або зупинення ліцензій та інших дозволів, одержання (наявність) яких є умовою для здійснення певного виду діяльності, зокрема, анулювання чи зупинення дії спеціальних дозволів на користування надрами; 7) заборона участі у приватизації, оренді державного майна резидентами іноземної держави та особами, які прямо чи опосередковано контролюються резидентами іноземної держави або діють в їх інтересах; 8) заборона користування радіочастотним ресурсом України; 9) обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування; 10) заборона здійснення публічних закупівель товарів, робіт і послуг у юридичних осіб-резидентів іноземної держави державної форми власності та юридичних осіб, частка статутного капіталу яких знаходиться у власності іноземної держави, а також публічних закупівель у інших суб'єктів господарювання, що здійснюють продаж товарів, робіт, послуг походженням з іноземної держави, до якої застосовано санкції згідно з цим Законом; 11) заборона або обмеження заходження іноземних невійськових суден та військових кораблів до територіального моря України, її внутрішніх вод, портів та повітряних суден до повітряного простору України або здійснення посадки на території України; 12) повна або часткова заборона вчинення правочинів щодо цінних паперів, емітентами яких є особи, до яких застосовано санкції згідно з цим Законом; 13) заборона видачі дозволів, ліцензій Національного банку України на здійснення інвестицій в іноземну державу, розміщення валютних цінностей на рахунках і вкладах на території іноземної держави; 14) припинення видачі дозволів, ліцензій на ввезення в Україну з іноземної держави	4) prevention of capital outflows outside Ukraine; 5) suspension of economic and financial obligations; 6) revocation or suspension of licenses and other permits, obtaining (availability) of which are a condition for carrying out a certain type of activity, in particular, revocation or suspension of special permits for subsoil use; 7) prohibition of participation in privatisation, lease of state property by residents of a foreign state and persons who are directly or indirectly controlled by residents of a foreign state or act in their interests; 8) ban on the use of radio frequency resources of Ukraine; 9) restriction or termination of the provision of telecommunications services and the use of public telecommunications networks; 10) prohibition of public procurement of goods, works and services from legal entities-residents of a foreign state of state ownership and legal entities, the share of the authorised capital of which is owned by a foreign state, as well as public procurement from other business entities selling goods, works, services originating from a foreign state to which sanctions have been applied in accordance with this Law; 11) prohibition or restriction of entry of foreign non-military vessels and warships into the territorial sea of Ukraine, its inland waters, ports and aircraft into the airspace of Ukraine or landing on the territory of Ukraine; 12) complete or partial prohibition of transactions in securities, the issuers of which are persons to whom sanctions have been applied in accordance with this Law; 13) prohibition of issuing permits, licenses of the National Bank of Ukraine for investments in a foreign state, placement of currency values on accounts and deposits in the territory of a foreign state; 14) termination of issuance of permits, licenses for import to Ukraine from a foreign state or export from Ukraine of currency values and restriction of issuance

чи вивезення з України валютних цінностей та обмеження видачі готівки за платіжними картками, емітованими резидентами іноземної держави; 15) заборона здійснення Національним банком України реєстрації учасника міжнародної платіжної системи, платіжною організацією якої є резидент іноземної держави; 16) заборона збільшення розміру статутного капіталу господарських товариств, підприємств, у яких резидент іноземної держави, іноземна держава, юридична особа, учасником якої є нерезидент або іноземна держава, володіє 10 і більше відсотками статутного капіталу або має вплив на управління юридичною особою чи її діяльність; 17) запровадження додаткових заходів у сфері екологічного, санітарного, фітосанітарного та ветеринарного контролю; 18) припинення дії торговельних угод, спільних проектів та промислових програм у певних сферах, зокрема у сфері безпеки та оборони; 19) заборона передання технологій, прав на об'єкти права інтелектуальної власності; 20) припинення культурних обмінів, наукового співробітництва, освітніх та спортивних контактів, розважальних програм з іноземними державами та іноземними юридичними особами; 21) відмова в наданні та скасування віз резидентам іноземних держав, застосування інших заборон в'їзду на територію України; 22) припинення дії міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України; 23) анулювання офіційних візитів, засідань, переговорів з питань укладення договорів чи угод; 24) позбавлення державних нагород України, інших форм відзначення; 25) інші санкції, що відповідають принципам їх застосування, встановленим цим Законом.	of cash on payment cards issued by residents of a foreign state; 15) prohibition of registration by the National Bank of Ukraine of a participant in an international payment system, the payment organisation of which is a resident of a foreign state; 16) prohibition to increase the authorised capital of companies, enterprises in which a resident of a foreign state, foreign state, legal entity, a member of which is a non-resident or foreign state, owns 10 percent or more of the authorised capital or has influence on management of the legal entity or its activities; 17) introduction of additional measures in the field of ecological, sanitary, phytosanitary and veterinary control; 18) termination of trade agreements, joint projects and industrial programs in certain areas, in particular in the field of security and defense; 19) prohibition of transfer of technologies, rights to objects of intellectual property rights; 20) termination of cultural exchanges, scientific cooperation, educational and sports contacts, entertainment programs with foreign states and foreign legal entities; 21) refusal to issue and cancel visas to residents of foreign countries, application of other bans on entry into the territory of Ukraine; 22) termination of international agreements, the binding nature of which has been approved by the Verkhovna Rada of Ukraine; 23) cancellation of official visits, meetings, negotiations on the conclusion of contracts or agreements; 24) deprivation of state awards of Ukraine, other forms of celebration; 25) other sanctions that comply with the principles of their application established by this Law.

Частина 1 статті 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення»: 1. Порядок функціонування електронної системи охорони здоров'я затверджується Кабінетом Міністрів України з урахуванням вимог законодавства про захист персональних даних.	Part 1 of the Article 11 of the Law of Ukraine 'On the medial financial state guarantees': 1. The e-Health Functioning Procedure is approved by the Cabinet of Ministers, considering the requirements of the legislation on protection of personal data.
Пункт 30 Постанови Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я»: 30. Заява пацієнта (його законного представника) про відкликання заяви про надання згоди на обробку персональних даних або про надання доступу третім особам до інформації, що міститься у центральній базі даних, повинна бути опрацьована протягом трьох робочих днів.	Part 30 of the Decree of the Cabinet of Ministers of Ukraine 'Some Aspects of e-Health': 30. A patient's (or his/her authorised representative) request to revoke his/her consent to personal data processing or giving third parties access to data from the central database must be processed in 3 business days.
Стаття 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини»: Суди застосовують при розгляді справ Конвенцію та практику Суду як джерело права.	Article 17 of the Law of Ukraine 'On the Enforcement of Decisions and the Application of the Case Law of the European Court of Human Rights': Courts use the European Convention on Human Rights and the case law of the European Court of Human Rights as a source of law.
Частина 5 статті 19 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини»: Міністерства, інші центральні органи виконавчої влади забезпечують систематичний контроль за додержанням у рамках відомчого підпорядкуванняадміністративної практики, що відповідає Конвенції та практиці Суду.	Part 5 of Article 19 of the Law of Ukraine 'On the Enforcement of Decisions and the Application of the Case Law of the European Court of Human Rights': Ministries, other central executive bodies shall provide systematic monitoring of the public practice compliance within their competence with the Convention and the Court's case law.
Стаття 15 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема	Article 15 of the Action Plan on the Implementation of the Association Agreement between the European Union, the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part: The Parties agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards,

відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, inter alia, обмін інформацією та експертами.	including the relevant Council of Europe instruments. Cooperation on personal data protection may include, inter alia, the exchange of information and of experts.
Пункт 11 Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затвердженого: 11.Удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679.	Article 11 of the Action Plan on the Implementation of the Association Agreement between the European Union, the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part: 11. Improvement of legislation on the protection of personal data in compliance with the Regulation (EC) 2016/679.

Bibliography

English titles

Legislation

Constitution of Ukraine 1996 <https://zakon.rada.gov.ua/laws/show/254к/96-вр/ed20200101>

Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part
<https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf>

The Civil Code of Ukraine 2003 №435-IV
<https://zakon.rada.gov.ua/laws/show/435-15>

The Criminal Code of Ukraine 2001 №2341-III
<https://zakon.rada.gov.ua/laws/show/2341-14>

The Law of Ukraine 'On Television and Radio Broadcasting' 1993 №3759-XII
<https://zakon.rada.gov.ua/laws/show/3759-12>

The Law of Ukraine 'On News Agencies' 1995 №74/95-ВР
<https://zakon.rada.gov.ua/laws/show/74/95-вр>

The Law of Ukraine 'On Information' 1992 №2657-XII
<https://zakon.rada.gov.ua/laws/show/2657-12>

The Law of Ukraine 'On Printed Mass Media (Press)' 1993 №2782-XII
<https://zakon.rada.gov.ua/laws/show/2782-12>

The Law of Ukraine 'On Personal Data Protection' 2010 №2297-VI
<https://zakon.rada.gov.ua/laws/show/2297-17>

The Law of Ukraine 'On State Statistics' 1992 №2614-XII
<https://zakon.rada.gov.ua/laws/show/2614-12>

The Law of Ukraine 'On Access to Public Information' 2011 №2939-VI
<https://zakon.rada.gov.ua/laws/show/2939-17>

The Law of Ukraine 'On State Classified Information' 1994 №3855-XII
<https://zakon.rada.gov.ua/laws/show/3855-12>

The Law of Ukraine 'On Banks and Banking Activity' 2000 №2121-III
<https://zakon.rada.gov.ua/laws/show/2121-14>

The Law of Ukraine 'On Sanctions' 2014 №1644-VII <https://zakon.rada.gov.ua/laws/show/1644-18>

The Law of Ukraine 'On the National Security and Defence Council of Ukraine' 1998 №183/98-ВР <https://zakon.rada.gov.ua/laws/show/183/98-вр>

The Law of Ukraine 'On Telecommunications' 2003 №1280-IV <https://zakon.rada.gov.ua/laws/show/1280-15>

The Law of Ukraine 'On the Protection of Public Morale' 2003 №1296-IV <https://zakon.rada.gov.ua/laws/show/1296-15>

The Law of Ukraine 'On Cinematography' 1998 №9/98-ВР <https://zakon.rada.gov.ua/laws/show/9/98-вр>

The Law of Ukraine 'On Copyright and Related Rights' 1993 №3792-XII<https://zakon.rada.gov.ua/laws/show/3792-12>

The Law of Ukraine 'On Electronic Commerce' 2015 №675-VII <https://zakon.rada.gov.ua/laws/show/675-19>

The Law of Ukraine 'On the Principles of Prevention and Combating Discrimination in Ukraine' 2012 №5207-VI <https://zakon.rada.gov.ua/laws/show/5207-17>

Model instruction on the procedure for keeping records, storing, using and destroying documents as well as other tangible information storage media containing official information as approved by the Cabinet's of Ministers Resolution as of 19 October 2016 №736 <https://zakon.rada.gov.ua/laws/show/736-2016-п>

Decree of the Cabinet of Ministers of Ukraine 'On the Liquidation of the National Expert Commission for the Protection of Public Morale' as of 27 May 2015 №333 <https://zakon.rada.gov.ua/laws/show/333-2015-п>

Procedure regarding Electronic Healthcare System Functioning as approved by the Decree of the Cabinet of Ministers of Ukraine 'On Some Aspects of e-Health' as of 2 April 2018 №411 <https://zakon.rada.gov.ua/laws/show/411-2018-п>

Action Plan on the Implementation of the Association Agreement between the European Union and its Member States, on the one hand, and Ukraine, on the other hand, approved by the Decree of the Cabinet of Ministers as of 25 October 2017 №1106 <https://zakon.rada.gov.ua/laws/show/1106-2017-п>

Decree of the President of Ukraine 'On the decision of the National Security and Defence Council 'On the Doctrine of Information Security of Ukraine' as of 29 December 2016 №47/2017 <https://zakon.rada.gov.ua/laws/show/47/2017/>

Decree of the President of Ukraine 'On the decision of the National Security and Defence Council of Ukraine as of 28 April 2017 'On the application of personal special economic and other restrictive measures (sanctions)' as of 15 May 2017 №133/2017 <https://zakon.rada.gov.ua/laws/show/ru/133/2017/>

Decree of the President of Ukraine 'On the decision of the National Security and Defence Council of Ukraine as of 26 November 2018 'On emergency measures to ensure state sovereignty and independence of Ukraine and the declaration of martial law in Ukraine' as of 26 November 2018 №390/2018
<https://zakon.rada.gov.ua/laws/show/390/2018>

Letter №36/1-5 as of 07 March 2017 on the implementation of the Decree of the President of Ukraine as of 25 February 2017 № 47/2017 (2017)
<https://inau.ua/document/lyst-no361-5-vid-07032017-shchodo-realizaciyi-ukazu-prezydenta-ukrayiny-vid-25022017-no>

Cybersecurity Strategy of Ukraine as enacted by the Decree of the President of Ukraine as of 15 March 2016 №96/2016 <https://zakon.rada.gov.ua/laws/show/96/2016>

Decision of the National Security and Defence Council of Ukraine as of 28 April 2017 <https://zakon.rada.gov.ua/laws/show/ru/n0004525-17/>

The list of legal entities sanctioned under the Decision of the National Security and Defence Council of Ukraine as of 28 April 2017, annexed to the Decision <https://zakon.rada.gov.ua/laws/file/text/54/f467150n25.pdf>

Decision On the appointment of unscheduled on-site inspection of LLC 'TRK '112-TV' №15 as of 09 January 2020
<https://www.nrada.gov.ua/wp-content/uploads/2020/01/R-2020-00015.pdf>

Reports

DW Akademie, #speakup barometer. 'Ukraine. Accessing Digital Participation' (2019) <https://www.dw.com/downloads/49486400/speakup-barometer-ukraine-full-report.pdf>

Olga Kyryliuk, 'Freedom of Expression in Times of Conflict: Ukrainian Realities. Analytical report' (2017)
<https://cedem.org.ua/wp-content/uploads/2017/08/Freedom-of-Expression_Report_Ukraine_DDP_ENG.pdf>

Freedom of the Net Report (2018)
<https://freedomhouse.org/country/ukraine/freedom-net/2018>

Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in 2019 (Secretariat of the Commissioner, 2020)
<http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf>

Yearly Report of the Ukrainian Parliament Commissioner for Human Rights on the State of Observance and Protection of Human and Citizens' Rights in Ukraine in 2017 (Secretariat of the Commissioner, 2018)
<http://www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf>

Freedom of the Net Report (2019)
<https://freedomhouse.org/country/ukraine/freedom-net/2019>

Books

Dmytro Kotliar, 'Scientific and Practical Commentary to the Law of Ukraine 'On Access to Public Information'' (Public Media Center, 2012)
<http://access-info.org.ua/wp-content/uploads/2015/12/205.pdf>

O. Burmagin, L. Opryshko, 'Freedom Of Speech On The Internet. A Practical Guide' (NGO 'Human Rights Platform', 2019)
<https://www.ppl.org.ua/wp-content/uploads/2019/02/СВОБОДА-СЛОВА-В-ІНТЕРНЕТІ.pdf>

A. Blaha, O. Martynenko, B. Mois, R. Shutov, 'Freedom of speech in times of information warfare and armed conflict'
<https://helsinki.org.ua/wp-content/uploads/2018/01/Web_Svoboda_Slova_A5_Ukr3.pdf>

Vita Volodovska, Maksym Drovovyi, 'Human Rights Online: Agenda for Ukraine' <https://dslua.org/wp-content/uploads/2019/12/DRA_FINAL_English.pdf>

Periodicals

Tetiana Prystupenko, 'The State of Legislative Regulation of Domestic Media in the Conditions of New History of Ukraine' (Scientific Notes of the Institute of Journalism, Volume 2 (67), 2017) 30 <http://nbuv.gov.ua/UJRN/Nzizh_2017_2_6>

Oksana Soldatenko, 'Information Space on the Internet: Legal Regulation and Control' (Entrepreneurship, Economy and Law, 2018) 138
<http://pgp-journal.kiev.ua/archive/2018/5/27.pdf>

Digital resources

Khrystyna Burtnyk, 'Confidential Information, Information about a Person and Personal Data: Correlation And Regulation',
<https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/>

Maksym Dvorovyi, 'How the Internet will be Regulated in Ukraine in 2017-2019. Risk Assessment and Recommendations'
<https://cedem.org.ua/analytics/ukraine-internet-regulation/>

The Draft Law 'On Media' №2693
<http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812>

'Representatives of Provider Associations Discussed the Draft Law of Ukraine 'On Media' with the Committee of Humanitarian and Information Policy'
<http://www.appk.org.ua/ru/news/show/predstavniki-asots%D1%96ats%D1%96i-provaider%D1%96v-obgovorili-z/page/4/>

Tetiana Adveieva, 'About the media law and the internet, or Regulate Unregulated'
<https://detector.media/rinok/article/174258/2020-01-28-pro-mediinii-zakon-ta-internet-abo-vregulyuvati-nevregulovane/>

Dr. Joan Barata Mir, Commissioned by the OSCE Representative on Freedom of the Media, 'Legal Analysis of the Draft Law Of Ukraine 'On Media'
<https://www.osce.org/representative-on-freedom-of-media/447508?download=true&fbclid=IwAR1n5cWdx8zGWTktJ4k-WmPEgNt9-azjZWsUICwJC0i-knMn840XCqmCTpI>

The Draft Law 'On Media in Ukraine' №2693-1
<http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67886>

'The Draft Law 'On media' is being examined by the Council of Europe'
<http://www.golos.com.ua/article/326485>

Conclusion on the Draft Law 'On Media in Ukraine'
<http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67886>

Committee of Freedom of speech supports the Draft Law 'On Media'
<https://yurincom.com/legal_news/komitet-z-pytan-svobody-slova-pidtrymav-proekt-zakonu-pro-media/>

Draft Law 'On the State Regulation of Activities Related to Organizing and Conducting Gambling' №2285-A
<http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67682>

Letter [by the Internet Association of Ukraine] № 05/1-5 as of 23 January 2020 to the Supreme Council on providing comments to the Draft Law 'On State Regulation of Activities Related to Organizing and Conducting Gambling' (№ 2285-A as of 18 December 2019)
<https://inau.ua/document/lyst-no-051-5-vid-23012020-vru-shchodo-nadannya-zauvazhen-do-zakonoproektu-pro-derzhavne>

The Draft Law 'On amendments to the Law of Ukraine 'On Consumer Protection' and some legislative acts of Ukraine on measures to de-shadow the activities of e-commerce entities' №6754 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62329>

'InAU proposes not to approve Draft Law №6754, which increases administrative pressure on Ukrainian business'
<https://inau.ua/news/inau-proponuye-ne-pogodzhuvaty-zakonoproekt-6754-yakyy-posylyuye-administratyvnyy-tysk-na>

The Draft Law 'On amendments to certain legislative acts of Ukraine about counteraction to threats to national security in the information sphere' №6688 5 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236>

'Coalition 'For Free Internet', Bill №6688 may lead to the complete cessation of some information resources'
<https://detector.media/infospace/article/139000/2018-07-02-zakonoproekt-6688-mozhe-prizvesti-do-povnogo-pripinennya-diyalnosti-deyakikh-informresursiv-koalitsiya-za-vilnii-internet/>

Alec Luhn, 'Ukraine blocks popular social networks as part of sanctions on Russia' <https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war>

'Freedom of speech vs. information security? Key quotes from UkraineWorld's event at Kyiv Security Forum 2019'
<https://netfreedom.org.ua/article/rozvagi-vidigrayut-znachno-bilshu-rol-u-viborchomu-procesi-nizh-racionalni-debati>

'Legal analysis of the presidential decree on blocking sites'
<https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html>

Dmytro Zolotukhin, 'Ukraine: FAQ on the Freedom of Speech Issues in Terms of Hybrid War' <https://medium.com/@postinformation/ukraine-faq-on-the-freedom-of-speech-issues-in-terms-of-hybrid-war-5370e84139b1>

Skarga, Official website of the Project <http://www.skarga.org.ua/>

'Internet Association of Ukraine signs memorandum of cooperation with NEC on Protection of Public Morale' <http://khpg.org/index.php?id=1237560807>

'InAU launches Skarga.ua project to eradicate violence on the Internet' <https://press.unian.ua/press/975381-inau-rozpochinae-proekt-skargaua-iz-vikorinennya-nasilstva-v-interneti.html>

'The Internet Association of Ukraine presented the key priorities of its security strategy in the field of information technology' <https://press.unian.ua/press/10869098-internet-asociaciya-ukrajini-predstavila-klyuchovi-prioriteti-svoyeji-strategiji-borotbi-za-bezpeku-u-sferi-informaciynih-tehnologiy-video.html>

Memorandum of the Information Initiative on Protection of Freedom of Speech <https://inau.ua/komitety/komitet-inau-z-pytan-zahystu-prav-lyudyny-ta-svobody-slova/memorandum-informaciynoyi>

'Provider Associations have published a Memorandum on the protection of minors in the provision of software services' <https://detector.media/rinok/article/106536/2015-04-28-asotsiatsii-provaideriv-oprilyudnili-memorandum-shchodo-zakhistu-nepovnolitnikh-pid-chas-nadannya-programnikh-poslug/>

Terms and procedure for providing telecommunication services by Ukrtelecom <https://ukrtelecom.ua/upload/iblock/cfa/326d383d23eb968f7d7d4adb98735867.pdf>

Terms of telecommunications services by Kyivstar <https://cdn.kyivstar.ua/sites/default/files/about/umovi_nadannya_telekomunikacinyih_poslug_ukr.pdf?_ga=2.202316242.23168176.1581423165-1385753686.1581423165>

'Recommendations of the Council on Freedom of Speech and Protection of Journalists under the President of Ukraine on the Bill on Countering Disinformation' <https://detector.media/infospace/article/174473/2020-02-04-rekomendatsii-ra

'Comparative table to the Draft Law of Ukraine 'On making amendments to certain legislative acts of Ukraine on ensuring national informational security and right of access

to reliable information' <https://detector.media/infospace/article/174057/2020-01-21-porivnyalna-tablitsya-do-proektu-zakonu-ukraini-pro-vnesennya-zmin-do-deyakikh-zakonodavchikh-aktiv-ukraini-shchodo-zabezpechennya-natsionalnoi-informatsiinoi-bezpeki-ta-prava-na-dostup-do-dostovirnoi-informatsii/>
Draft Law 'On Media' №2693
<https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812>

Maryna Dorosh, 'Hate speech - new manifestations and consequences' (2015) <https://ms.detector.media/zakonodavstvo/post/12829/2015-03-17-mova-vorozhnechi-novi-proyavi-ta-naslidki/>

OSCE, Comparative Legal Analysis of Ukrainian Regulation of Hate Speech in the Media <https://www.osce.org/fom/371841?download=true>

State Court Administration, Official website
<https://court.gov.ua/inshe/sudova_statystyka/>

L. Opryshko, V. Volodovska, M. Drovovyi, 'Freedom of Expression on the Internet: Legislative Initiatives and Practice of Examination of Criminal Cases in Ukraine in 2014-2018' <https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf>

Prosecutor General's Office of Ukraine <https://old.gp.gov.ua/ua/stst2011.html>

Amnesty International, 'Ukraine: A year after attack on Roma camp in Kyiv, no justice for victims' <https://www.amnesty.org/en/latest/news/2019/04/ukraine-a-year-after-attack-on-roma-camp-in-kyiv-no-justice-for-victims/>

Human Rights Watch, 'Joint Letter to Ukraine's Minister of Interior Affairs and Prosecutor General Concerning Radical Groups'
<https://www.hrw.org/news/2018/06/14/joint-letter-ukraines-minister-interior-affairs-and-prosecutor-general-concerning>

Human Rights Watch, 'Ukraine. Event of 2019' <https://www.hrw.org/world-report/2020/country-chapters/ukraine>

'112 Ukraine' statement on the next fact of censorship by the National Council of Ukraine on Television and Radio' <https://tv-ua.112.ua/novyny-kanalu/zaiava-112-ukraina-z-pryvodu-cherhovoho-faktu-tsenzury-z-boku-natsrady-z-tb-521342.html>

'Maxi-TV is subject to sanctions of 'warning' and 'fine' in the amount of more than one hundred thousand hryvnias for the spread of hate speech'

<https://www.nrada.gov.ua/telekompaniyi-maksi-tv-zastosovano-sanktsiyi-ogoloshennya-poperedzhennya-ta-styagnennya-shtrafu-v-sumi-ponad-sto-tysyach-gryven-za-poshyrennya-movy-vorozhnechi/>

'NewsOne should pay over UAH 95,000 for hate speech' <https://www.nrada.gov.ua/telekanal-newsone-povynen-splatyty-shtraf/>
Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence <https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf>

Tetiana Bondarenko, 'Hate speech: how the Ukrainian media neglects journalistic standards' <http://detector.media/infospace/article/128539/2017-07-05-mova-vorozhnechi-yak-ukrainski-zmi-nekhtuyut-zhurnalistskimi-standartami/>

Institute of Mass Information, 'Analysis of the so-called mass media of 'DNR' and 'LNR': in every tenth piece of news – hate speech towards Ukrainians, 11% of news are fakes' <https://imi.org.ua/news/analiz-internet-zmi-tzv-dnr-ta-lnr-u-kojniy-desyatiy-novini-mova-vorojnechi-schodo-ukrajintsiv-11-i17084>

'Which right has priority: the right to freedom of speech or the right to privacy?' <https://www.ppl.org.ua/bibliotech/2-2>

Andrii Paziuk, 'Privacy and the Internet' <http://khpg.org/index.php?id=968016432>

Reporters without borders, 'Ukraine' <https://rsf.org/en/ukraine>

Freedom House, 'Should Ukraine Drop Sanctions against Russian Tech Companies?': <https://freedomhouse.org/report/policy-brief/2019/should-ukraine-drop-sanctions-against-russian-tech-companies>

Case law

The Resolution of the Constitutional Court of Ukraine 2012 № 2-рп/2012 <https://zakon.rada.gov.ua/laws/show/v002p710-12>

Resolution of the Constitutional Court of Ukraine 1997 № 5-зп <https://zakon.rada.gov.ua/laws/show/v005p710-97>

The Sunday Times v. *the United Kingdom*, no. 6538/74<http://hudoc.echr.coe.int/eng?i=001-57584>

Case №П/800/217/17 (05 June 2019) <http://www.reyestr.court.gov.ua/Review/82738705>

Case №800/321/17 (13 June 2018) <www.reyestr.court.gov.ua/Review/75286971>

Case №800/205/17 (20 December 2018)
<www.reyestr.court.gov.ua/Review/78808026>

Case №2/686/2114/18 (04 December 2018)
<http://reyestr.court.gov.ua/Review/78885244>

Case №2/640/1194/17 (29 May 2017)
<http://reyestr.court.gov.ua/Review/66893382>

Case №2/0274/820/15 (11 December 2015)
<http://reyestr.court.gov.ua/Review/54274488>

Case №577/2983/19 (10 November 2019)
<http://reyestr.court.gov.ua/Review/85705627>

Case №12685/19 (11 December 2019)
<http://reyestr.court.gov.ua/Review/86359546>

Case №296/418/15-c (29 March 2016)
<http://reyestr.court.gov.ua/Review/56849990>

Case №22-c/816/5062/19 (14 November 2019)
<http://reyestr.court.gov.ua/Review/85705627>

Case №520/4864/19 (11 December 2019)
<http://reyestr.court.gov.ua/Review/86359546>

Ukrainian titles

Legislation

Конституція України 1996 <https://zakon.rada.gov.ua/laws/show/254к/96-вр/ed20200101>

Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони
<https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf>

Цивільний кодекс України 2003 №435-IV
<https://zakon.rada.gov.ua/laws/show/435-15>

Кримінальний кодекс України 2001 №2341-III
<https://zakon.rada.gov.ua/laws/show/2341-14>

Закон України «Про телебачення і радіомовлення» 1993 №3759-XII
<https://zakon.rada.gov.ua/laws/show/3759-12>

Закон України «Про інформаційні агентства» 1995 №74/95-ВР
<https://zakon.rada.gov.ua/laws/show/74/95-вр>

Закон України «Про інформацію» 1992 №2657-XII
<https://zakon.rada.gov.ua/laws/show/2657-12>

Закон України «Про друковані засоби масової інформації (пресу) в Україні» 1993 №2782-XII <https://zakon.rada.gov.ua/laws/show/2782-12>

Закон України «Про захист персональних даних» 2010 №2297-VI
<https://zakon.rada.gov.ua/laws/show/2297-17>

Закон України «Про державну статистику» 1992 №2614-XII
<https://zakon.rada.gov.ua/laws/show/2614-12>

Закон України «Про доступ до публічної інформації» 2011 №2939-VI
<https://zakon.rada.gov.ua/laws/show/2939-17>

Закон України «Про державну таємницю» 1994 №3855-XII
<https://zakon.rada.gov.ua/laws/show/3855-12>

Закон України «Про банки і банківську діяльність» 2000 №2121-III
<https://zakon.rada.gov.ua/laws/show/2121-14>

Закон України «Про санкції» 2014 №1644-VII
<https://zakon.rada.gov.ua/laws/show/1644-18>

Закон України «Про раду національної безпеки і оборони України» 1998 №183/98-ВР <https://zakon.rada.gov.ua/laws/show/183/98-вр>

Закон України «Про телекомунікації» 2003 №1280-IV
<https://zakon.rada.gov.ua/laws/show/1280-15>

Закон України «Про захист суспільної моралі» 2003 №1296-IV
<https://zakon.rada.gov.ua/laws/show/1296-15>

Закон України «Про кінематографію» 1998 №9/98-ВР
<https://zakon.rada.gov.ua/laws/show/9/98-вр>

Закон України «Про авторське право і суміжні права» 1993 №3792-XII
<https://zakon.rada.gov.ua/laws/show/3792-12>

Закон України «Про електронну комерцію» 2015 №675-VII
<https://zakon.rada.gov.ua/laws/show/675-19>

Закон України «Про засади запобігання та протидії запобігання дискримінації в Україні» 2012 №5207-VI <https://zakon.rada.gov.ua/laws/show/5207-17>

Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету Міністрів України від 16 жовтня 2016 №736 <https://zakon.rada.gov.ua/laws/show/736-2016-п>

Постанова Кабінету Міністрів України «Про ліквідацію Національної експертної комісії з питань захисту суспільної моралі» від 27 травня 2015 №333 <https://zakon.rada.gov.ua/laws/show/333-2015-п>

Порядок функціонування електронної системи охорони здоров'я, затверджений Постановою Кабінету Міністрів України від «Деякі питання електронної системи охорони здоров'я» від 2 квітня 2018 №411
<https://zakon.rada.gov.ua/laws/show/411-2018-п>

План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затверджений Постановою Кабінету Міністрів України від 25 жовтня 2017 №1106
<https://zakon.rada.gov.ua/laws/show/1106-2017-п>

Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про доктрину інформаційної безпеки України» від 29 грудня 2016 №47/2017 <https://zakon.rada.gov.ua/laws/show/47/2017/>

Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 15 травня 2017 №133/2017 <https://zakon.rada.gov.ua/laws/show/ru/133/2017/>

Указ Президента України «Про рішення Ради національної безпеки і оборони України від 26 листопада 2018 «Щодо надзвичайних заходів із забезпечення державного суверенітету і незалежності України та введення воєнного стану в Україні» від 26 листопада 2018 №390/2018
<https://zakon.rada.gov.ua/laws/show/390/2018>

Лист [Інтернет Асоціації України] №36/1-5 від 07.03.2017 щодо реалізації Указу Президента України від 25.02.2017 №47/2017 <https://inau.ua/document/lyst-no361-5-vid-07032017-shchodo-realizaciyi-ukazu-prezydenta-ukrayiny-vid-25022017-no>

Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 №96/2016 <https://zakon.rada.gov.ua/laws/show/96/2016>

Рішення Ради національної безпеки і оборони України від 28 квітня 2017 <https://zakon.rada.gov.ua/laws/show/ru/n0004525-17/>

Юридичні особи, до яких застосовуються обмежувальні заходи (санкції), відповідно до Рішення Ради національної безпеки і оборони України від 28 квітня 2017 <https://zakon.rada.gov.ua/laws/file/text/54/f467150n25.pdf>

Рішення Національної ради України з питань телебачення і радіомовлення «Про призначення позапланової виїзної перевірки ТОВ «ТРК «112-ТВ» №15 від 9 січня 2020 <https://www.nrada.gov.ua/wp-content/uploads/2020/01/R-2020-00015.pdf>

Reports

DW Akademie, #speakup barometer. «Україна. Оцінюючи цифрове залучення» <https://www.dw.com/downloads/49486400/speakup-barometer-ukraine-full-report.pdf>

Ольга Кирилюк, «Свобода думки у часи конфлікту: українські реалії. Аналітичний звіт» (2017)
<https://cedem.org.ua/wp-content/uploads/2017/08/Freedom-of-Expression_Report_Ukraine_DDP_ENG.pdf>

Звіт Freedom of the Net, 2018
<https://freedomhouse.org/country/ukraine/freedom-net/2018>

Щорічна доповідь Уповноваженого Верховної Ради з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2019 (Секретаріат Уповноваженого, 2020)
<http://www.ombudsman.gov.ua/files/Dopovidi/zvit%20za%202019.pdf>

Щорічна доповідь Уповноваженого Верховної Ради з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2017 (Секретаріат Уповноваженого, 2018)
<http://www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf>

Звіт Freedom of the Net 2019 <https://freedomhouse.org/country/ukraine/freedom-net/2019>

Л. Опришко, В. Володовська, М. Дворовий, «Свобода слова в Інтернеті: Законодавчі ініціативи та практики розгляду кримінальних справ в Україні 2014-2018» <https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf>

Books

Дмитро Котляр, «Науково-практичний коментар до Закону України «Про доступ до публічної інформації» (Центр суспільних медіа, 2012) <http://access-info.org.ua/wp-content/uploads/2015/12/205.pdf>

О. Бурмагін, Л. Опришко, «Свобода слова в Інтернеті: практичний посібник» (ГО «Платформа прав людини», 2019)
<https://www.ppl.org.ua/wp-content/uploads/2019/02/СВОБОДА-СЛОВА-В-ІНТЕРНЕТІ.pdf>

А. Блага, О. Мартиненко, Б. Мойса, Р, Шутов, «Свобода слова в умовах інформаційної війни та збройного конфлікту» <https://helsinki.org.ua/wp-content/uploads/2018/01/Web_Svoboda_Slova_A5_Ukr3.pdf>

Віта Володовська, Максим Дворовий, «Порядок денний для України: цифрові права»
<https://dslua.org/wp-content/uploads/2019/12/DRA_FINAL_English.pdf>

Periodicals

Тетяна Приступенко, «Стан законодавчого регулювання вітчизняних ЗМІ в умовах новітньої історії України» (Наукові записки Інституту журналістики, Том 2 (67), 2017) 30 <http://nbuv.gov.ua/UJRN/Nzizh_2017_2_6>

Оксана Солдатенко, «Інформаційний простір в мережі Інтернет: правове регулювання та контроль» (Підприємництво, господарство і право, 2018) 138 <http://pgp-journal.kiev.ua/archive/2018/5/27.pdf>

Digital resources

Христина Буртник, «Конфіденційна інформація, інформація про особу та персональні дані: співвідношення і регулювання» <https://cedem.org.ua/analytics/konfidentsijna-informatsiya-informatsiya-pro-osobu-ta-personalni-dani-spivvidnoshennya-i-regulyuvannya/>

Максим Дворовий, «Як регулюватиметься Інтернет в Україні в 2017-2019 роках. Оцінка ризиків та рекомендації» <https://cedem.org.ua/analytics/ukraine-internet-regulation/>

Проект Закону «Про медіа» №2693 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812>

«Представники асоціацій провайдерів обговорили з керівництвом комітета гуманітарної та інформаційної політики Проект Закону України «Про медіа» <http://www.appk.org.ua/ru/news/show/predstavniki-asots%D1%96ats%D1%96i-provaider%D1%96v-obgovorili-z/page/4/>

Тетяна Авдєєва, «Про медійний закон та Інтернет, або Врегулювати неврегульоване» <https://detector.media/rinok/article/174258/2020-01-28-pro-mediinii-zakon-ta-internet-abo-vregulyuvati-nevregulovane/>

Доктор Джоан Барата Мір га замовлення Представника ОБСЄ зі свободи медіа, «Правовий аналіз Проекту Закону України «Про медіа» <https://www.osce.org/representative-on-freedom-of-media/447508?download=true&fbclid=IwAR1n5cWdx8zGWTktJ4k-WmPEgNt9-azjZWsUICwJC0i-knMn840XCqmCTpI>

Проект Закону України «Про медіа в Україні» №2693-1 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67886>

«Проект закону «Про медіа» проходить експертизу в Раді Європи» <http://www.golos.com.ua/article/326485>

Висновок щодо Закону України «Про медіа в Україні» <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67886>

Комітет Свободи слова підтримує Проект Закону «Про медіа» <https://yurincom.com/legal_news/komitet-z-pytan-svobody-slova-pidtrymav-proekt-zakonu-pro-media/>

Проект Закону «Про державне регулювання діяльності щодо організації та проведення азартних ігор» №2285-д <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67682>

Лист № 05/1-5 від 23.01.2020 ВРУ щодо надання зауважень до законопроекту «Про державне регулювання діяльності щодо організації та проведення азартних ігор» (реєстр. № 2285-д від 18.12.2019) <https://inau.ua/document/lyst-no-051-5-vid-23012020-vru-shchodo-nadannya-zauvazhen-do-zakonoproektu-pro-derzhavne>

Проект Закону про внесення змін до Закону України «Про захист прав споживачів» та деяких законодавчих актів України щодо заходів детінізації діяльності суб'єктів електронної комерції №6754 <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62329>

«ІнАУ пропонує не погоджувати законопроект 6754, який посилює адміністративний тиск на український бізнес» <https://inau.ua/news/inau-proponuye-ne-pogodzhuvaty-zakonoproekt-6754-yakyy-posylyuye-administratyvnyy-tysk-na>

Проект Закону про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері <http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236>

«Законопроект №6688 може призвести до повного припинення діяльності деяких інформресурсів – Коаліція «За вільний Інтернет» <https://detector.media/infospace/article/139000/2018-07-02-zakonoproekt-6688-mozhe-prizvesti-do-povnogo-pripinennya-diyalnosti-deyakikh-informresursiv-koalitsiya-za-vilnii-internet/>

Алек Лун, «Україна блокує популярні соціальні мережі як частина санкцій щодо Росії» <https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war>

«Свобода слова проти інформаційної безпеки? Ключові цитати UkraineWorld's Київського форуму безпеки 2019» <https://netfreedom.org.ua/article/rozvagi-vidigrayut-znachno-bilshu-rol-u-viborchomu-procesi-nizh-racionalni-debati>

«Юридичний аналіз Указу Президента про блокування сайтів» <https://www.ppl.org.ua/yuridichnij-analiz-ukazu-prezidenta-pro-blokuvannya-sajtiv.html>

Дмитро Золотихін, «Україна: відповіді на часті питання щодо свободи слова у часи гібридної війни» <https://medium.com/@postinformation/ukraine-faq-on-the-freedom-of-speech-issues-in-terms-of-hybrid-war-5370e84139b1>

Скарга, Офіційний сайт проекту <http://www.skarga.org.ua/>

«Інтернет-асоціація України підписала меморандум про співробітництво з НЕК з питань захисту суспільної моралі» <http://khpg.org/index.php?id=1237560807>

«ІнАУ розпочинає проект Skarga.ua із викорінення насильства в Інтернеті» <https://press.unian.ua/press/975381-inau-rozpochinae-proekt-skargaua-iz-vikorinennya-nasilstva-v-interneti.html>

«Інтернет Асоціація України представила ключові пріоритети своєї стратегії боротьби за безпеку у сфері інформаційних технологій (відео)» <https://press.unian.ua/press/10869098-internet-asociaciya-ukrajini-predstavila-klyuchovi-prioriteti-svoyeji-strategiji-borotbi-za-bezpeku-u-sferi-informaciynih-tehnologiy-video.html>

Меморандум Інформаційної ініціативи з питань захисту свободи слова <https://inau.ua/komitety/komitet-inau-z-pytan-zahystu-prav-lyudyny-ta-svobody-slova/memorandum-informaciynoyi>

«Асоціації провайдерів оприлюднили Меморандум щодо захисту неповнолітніх під час надання програмних послуг» <https://detector.media/rinok/article/106536/2015-04-28-asotsiatsii-provaideriv-oprilyudnili-memorandum-shchodo-zakhistu-nepovnolitnikh-pid-chas-nadannya-programnikh-poslug/>

Умови та порядок надання телекомунікаційних послуг ПАТ «Укртелеком» <https://ukrtelecom.ua/upload/iblock/cfa/326d383d23eb968f7d7d4adb98735867.pdf>

Умови надання телекомунікаційних послуг приватного акціонерного товариства «Київстар» <https://cdn.kyivstar.ua/sites/default/files/about/umovi_nadannya_telekomunikacinih_poslug_ukr.pdf?_ga=2.202316242.23168176.1581423165-1385753686.1581423165>

«Рекомендації Ради з питань свободи слова та захисту журналістів при президентові України щодо законопроєкту про протидію дезінформації» <https://detector.media/infospace/article/174473/2020-02-04-rekomendatsii-ra

«Порівняльна таблиця до проєкту Закону України «Про внесення змін до деяких законодавчих актів України щодо забезпечення національної інформаційної безпеки та права на доступ до достовірної інформації» <https://detector.media/infospace/article/174057/2020-01-21-porivnyalna-tablitsya-do-proektu-zakonu-ukraini-pro-vnesennya-zmin-do-deyakikh-zakonodavchikh-aktiv-ukraini-shchodo-zabezpechennya-natsionalnoi-informatsiinoi-bezpeki-ta-prava-na-dostup-do-dostovirnoi-informatsii/>

Проект Закону «Про медіа» №2693 <https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812>

Марина Дорош, «Мова ворожнечі – нові прояви та наслідки» (2015) <https://ms.detector.media/zakonodavstvo/post/12829/2015-03-17-mova-vorozhnechi-novi-proyavi-ta-naslidki/>

ОБСЄ, «Порівняльний юридичний аналіз правового регулювання мови ворожнечі в медіа в Україні» <https://www.osce.org/fom/371841?download=true>

Судова влада України, Офіційний сайт <https://court.gov.ua/inshe/sudova_statystyka/>

Генеральна прокуратура України <https://old.gp.gov.ua/ua/stst2011.html>

Amnesty International, «Україна: Рік по атаці на табір Roma у Києві, ніякої справедливості для потерпілих» <https://www.amnesty.org/en/latest/news/2019/04/ukraine-a-year-after-attack-on-roma-camp-in-kyiv-no-justice-for-victims/>

Human Rights Watch, «Спільний лист до Міністра Внутрішніх справ України та Генерального прокурора України стосовно радикальних груп» <https://www.hrw.org/news/2018/06/14/joint-letter-ukraines-minister-interior-affairs-and-prosecutor-general-concerning>

Human Rights Watch, «Україна. Події 2019» <https://www.hrw.org/world-report/2020/country-chapters/ukraine>

«Заява «112 Україна» з приводу чергового факту цензури з боку Нацради з питань ТБ»
<https://tv-ua.112.ua/novyny-kanalu/zaiava-112-ukraina-z-pryvodu-cherhovoho-faktu-tsenzury-z-boku-natsrady-z-tb-521342.html>

«До телекомпанії «Максі-ТВ» застосовано санкції «оголошення попередження» та «стягнення штрафу» на суму понад сто тисяч гривень за поширення мови ворожнечі»
<https://www.nrada.gov.ua/telekompaniyi-maksi-tv-zastosovano-sanktsiyi-ogoloshennya-poperedzhennya-ta-styagnennya-shtrafu-v-sumi-ponad-sto-tysyach-gryven-za-poshyrennya-movy-vorozhnechi/>

«Телеканал «NewsOne» повинен сплатити штраф понад 95 тисяч гривень за мову ворожнечі»
<https://www.nrada.gov.ua/telekanal-newsone-povynen-splatyty-shtraf/>

План Рабат щодо Дій про заборону виступів за національну, расову чи релігійну ворожнечу що становить заклики до дискримінації, ворожнечі чи насилля' <https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf>

Тетяна Бондаренко, «Мова ворожнечі: як українські ЗМІ нехтують журналістськими стандартами»
<http://detector.media/infospace/article/128539/2017-07-05-mova-vorozhnechi-yak-ukrainski-zmi-nekhtuyut-zhurnalistskimi-standartami/>

Інститут масової інформації, «Аналіз інтернет-ЗМІ т.зв. «ДНР» та «ЛНР»: у кожній десятій новині — мова ворожнечі щодо українців, 11% новин — фейки» <https://imi.org.ua/news/analiz-internet-zmi-tzv-dnr-ta-lnr-u-kojniy-desyatiy-novini-mova-vorojnechi-schodo-ukrajintsiv-11-i17084>

«Яке право має пріоритет: право на свободу слова чи право на приватність?» <https://www.ppl.org.ua/bibliotech/2-2>

Андрій Пазюк, «Приватність та Інтернет»
<http://khpg.org/index.php?id=968016432>

Reporters without borders, «Україна» <https://rsf.org/en/ukraine>

Freedom House, «Чи має Україна зняти санкції щодо технологічних компаній Росії?» <https://freedomhouse.org/report/policy-brief/2019/should-ukraine-drop-sanctions-against-russian-tech-companies>

Case law

Рішення Конституційного суду України 2012 № 2-рп/2012 <https://zakon.rada.gov.ua/laws/show/v002p710-12>

Рішення Конституційного суду України 1997 № 5-зп <https://zakon.rada.gov.ua/laws/show/v005p710-97>

Санді Таймс п. *Сполученого Королівства*, №. 6538/74 <http://hudoc.echr.coe.int/eng?i=001-57584>

Справа №П/800/217/17 (05 червня 2019) <http://www.reyestr.court.gov.ua/Review/82738705>

Справа №800/321/17 (13 червня 2018) <www.reyestr.court.gov.ua/Review/75286971>

Справа №800/205/17 (20 грудня 2018) <www.reyestr.court.gov.ua/Review/78808026>

Справа №2/686/2114/18 (04 грудня 2018) <http://reyestr.court.gov.ua/Review/78885244>

Справа №2/640/1194/17 (29 травня 2017) <http://reyestr.court.gov.ua/Review/66893382>

Справа №2/0274/820/15 (11 грудня 2015) <http://reyestr.court.gov.ua/Review/54274488>

Справа №577/2983/19 (10 листопада 2019) <http://reyestr.court.gov.ua/Review/85705627>

Справа №12685/19 (11 грудня 2019) <http://reyestr.court.gov.ua/Review/86359546>

Справа №296/418/15-с (29 березня 2016) <http://reyestr.court.gov.ua/Review/56849990>

Справа №22-с/816/5062/19 (14 листопада 2019) <http://reyestr.court.gov.ua/Review/85705627>

Справа №520/4864/19 (11 грудня 2019) <http://reyestr.court.gov.ua/Review/86359546>

ELSA United Kingdom

Contributors

National Coordinator

Dora Homanyi

National Researchers

Alejandra Rodriguez

Alexia Enriquez

Batuhan Öneş

Conor Courtney

Kasia Kotka

National Linguistic Editor

Connor Courtney

Acknowledgements

As the National Coordinator of ELSA United Kingdom, I would like to thank everyone who helped for this research to get published. Mainly to our amazing and hardworking researchers.

Introduction

The topic of the LRG, the internet censorship is one of the mostly talked topics at the moment. In the United Kingdom, and just generally throughout the world. The internet censorship, and freedom of expression are important and at the moment with all the technical improvement we need to address the arising issues and the challenges what we are facing. Every domestic legislation has different points and elements, what we need to address and compare the valid points to make sure we will reach a point where the legislation is at the best interest of all people.

1. How is freedom of expression protected in your national legislation and which legislation is in place to protect against limitation towards freedom of expression?

1.1 Freedom of Expression

It is a tough balance to strike between safeguarding and surveillance. This balance has become increasingly difficult in a time where the Internet has gained so much force and global reach. In the UK there are legislations set in place to help protect the fundamental Right of Freedom of Expression. The Human Rights Act of 1998 (HRA) put forth by the European Convention of Human Rights (ECHR) established a script by which the UK is able to provide relevant human rights such as: Article 9 on the Freedom of thought, conscience and religion, Article 10 on Freedom of Expression, as well as Article 14 on the prohibition of discrimination.[2253] The Internet adds a new dimension to this discussion, which can be very challenging for States to regulate while simultaneously respecting individuals' fundamental freedoms. In addition to the HRA 1998, the United Nations' Universal Declaration of Human Rights' (UDHR) Article 19 has also lent a helping hand in defining freedom of expression: 'this right includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any

[2253] Human Rights Act 1998, sched 1, art 9, 10 & 14.

media and regardless of frontiers.' [2254] More than just a fundamental freedom of expression, it is a human right that additionally 'enables the enjoyment of other human rights, including economic, social and cultural rights and civil and political rights, such as freedom of association and assembly.' [2255]

The Internet has become a place that has 'increased the visibility of hate speech, which has been made more acute by increases in immigration, social and economic turmoil and the emergence of terrorism.' [2256] As a result, 'the very nature of the Internet makes it easier for authors of hate speech to get their message of hate across and more difficult for authorities to fight it.' [2257] Article 10 of the HRA on Freedom of Expression has long been contested in light of the Internet as it comes into conflict with other aspects such as hate speech or mature/inappropriate content. In 2017, the UK passed a Bill called the Digital Economy Act on electronic communications and infrastructure, which requires Internet Service Providers (ISPs) to block inappropriate pornographic content that is inadequate for minors. [2258] As some understand it, it is crucial to 'comprehend the value inherent in free expression to understand why some of the current tensions between privacy and security on the one hand and free speech on the other exist [since] free expression is seen as a right that can legitimately be pitted against privacy and security.' [2259]

1.2 Freedom of Information

In 2000, the UK officially adopted a Parliamentary Act called the Freedom of Information Act, which gives individuals 'the right to ask to see recorded information held by public authorities […] you do not need to tell the organisation which law or regulations you're making your request under.' [2260] This Act is meant to give individuals the freedom and right to reach information through requests as a way to build on citizen's participation and trust towards the government through transparency and accountability. However, there is little evidence to demonstrate that the implementation of this Act has actually rectified the public's mistrust in the government's censorship on information.

[2254] Universal Declaration of Human Rights 1948.
[2255] Wolfgang Benedek and Matthias C. Kettemann, *Freedom of Expression and the Internet* (2013) Council of Europe Publishing, 79
[2256] ibid (n 2255) 83
[2257] ibid (n 2256) 82.
[2258] Digital Economy Act 2017 c.30
[2259] Jodie Ginsberg, 'Balancing Privacy and Free Expression Online' (June 2016), Infotoday, 5.
[2260] Gov.UK, *How to make a freedom of information (FOI) request*, Freedom of Information Act 2000, https://www.gov.uk/make-a-freedom-of-information-request

On a similar topic, as one of few States to do this, the UK has legislation set in place to protect whistle-blowers. According to the Council of Europe this solidifies individuals' rights under Article 10 of the HRA 1998 on the right to disclose information of public concern. [2261] Some believe that whistle-blowers should also be entitled to basic human rights due to their courageous acts of providing "an opportunity to strengthen accountability and bolster the right against corruption and mismanagement, both in the public and private sector." [2262] In putting legislations forward, the UK seeks to continue building on the nation's trust by providing the means necessary to afford everyone the right to information – whether they have been successful in transmitting this message across or not continues to be a subjective standpoint.

1.3 Restrictions on Freedom: Censorship

When boundaries are crossed, the concept of freedom of expression can be tamed by restrictions, interference and 'censorship through filtering or blocking of online content.' [2263] In the UK one of the most prominent examples of censorship is Part 3 of the Digital Economy Act of 2017, which seeks to completely censor and block pornographic content online for users under the age of 18 and is aiming to become stricter in the upcoming months.[2264]

Furthermore, there are still lingering restrictions on what can and cannot be published by news and media outlets based on the previous Official Secrets Act 1989. This Act established boundaries in terms of classified governmental intel, which seek to protect the UK from risks of espionage. [2265] More recently, the Terrorism Act of 2006 has also come into force as another piece of legislation that promotes online censorship, but this time in regards to terrorist glorification and praise for purposes of maintaining national security.[2266] Though many would agree that this is a proactive statute, some may see this is a way for the government to set limits on the fundamental freedom of speech. It is for this reason that any legitimate restriction will necessarily be subject to stringent requirements: they must 'be construed strictly' and their necessity 'established convincingly'. If there is legitimate reason for interference with the right, the interference must be 'necessary in a democratic society' and 'proportionate to

[2261] Wolfgang Benedek and Matthias C. Kettemann, *Freedom of Expression and the Internet* (2013) Council of Europe Publishing, 79(n 2256) 124.
[2262] ibid (n 2256) 124, 125.
[2263] ibid (n 2256) 45.
[2264] ibid (n 2258).
[2265] Official Secrets Act 1989, c.6.
[2266] Terrorism Act 2006, c. 11.

the legitimate aim pursued [as was seen in] the *Sunday Times vs the United Kingdom.*[2267]

As it has it, there seem to be discrepancies in the distinction between freedom of expression and the duty to protect because when expression turns into hate or violence, restrictions come into play.

1.4 Freedom vs. Protection

So, where does one draw the line between granting enough freedom while ensuring enough protection? There are two statutes that currently stand out in the UK that come into conflict with the extent to which freedom of expression may be exercised. First, the Racial and Religious Hatred Act of 2006, which amended the original Public Order Act 1986 has been put forth as a way to prohibit behaviour that incites discrimination or hate towards individuals based on their racial or religious background. [2268] While this may hinder the ability to express oneself freely, it also protects individuals from being discriminated against in society, which in and of itself is a fundamental human right, as per Article 14 of the HRA. In addition to the factors of race and religion, recent legislation has found a need to amend – through the Criminal Justice and Immigration Act of 2008 – Part 3A of the Public Order Act of 1986 so to also include hatred towards persons of distinct sexual orientations. [2269]

Second, the more recent English Defamation Act of 2013 touches on both the concepts of freedom of expression and the protection of reputation. This Act has been established in order to ensure that claims of defamation are probable and sufficiently serious to move forward in order to protect personal reputation rights. Under the Defamation Act of 2013, serious harm is classified as the following:

a statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant.

for the purpose of this section, harm to the reputation of a body that trades for profit is not "serious harm" unless it has caused or is likely to cause the body serious financial loss. [2270]

[2267] Daragh Murray, 'Freedom of Expression, Counter-Terrorism and the Internet in Light of the UK Terrorist Act 2006 and the Jurisprudence of the European Court of Human Rights' (2009) 27 Neth Q Hum Rts, 338.

[2268] Racial and Religious Hatred Act 2006, c. 1, section 1.

[2269] Criminal Justice and Immigration Act 2008, c.4, Part 5 Hatred on the grounds of sexual orientation.

[2270] Defamation Act 2013, c. 26, Section 1 Requirement of serious harm.

As it has it, there are aspects of the recent legislation that, although aiming to promote freedom of expression, they also limit the threshold of expression that can be exercised by restraining it to a given framework. Nevertheless, in doing so the aforementioned statues aim to find a balance between affording enough freedom of expression while still ensuring protection of all individuals and avoiding further concerns of hate speech and/or discrimination.

1.5 When Freedom is Misused

As many would agree, the 'internationalisation of discourses and the assessment of expression under different jurisdictions has made it difficult to find clear answers to the question of what content is (or should be) prohibited.' [2271] One of the main concerns with online/instant communication is the velocity at which hate speech can be expressed and/or spread. This is especially concerning in cases, such as the British case of *Handyside v UK*[2272], which included not only hateful but also shockingly offensive attitudes that can affect individuals in a very negative way.

With globalisation being such a predominant concept of the modern world, issues of hate speech are often brought into question when discussing the Internet. Although Article 14 of the HRA aims to protect all individuals against discrimination there are still a lot of issues relating to racism, xenophobia and homophobia that surface online. The current Mayor of London, Sadiq Khan, has been very vocal about the fact that change is needed in this field, in fact, he has 'publicly advocated for large fines to be applied to tech platforms that failed to remove hate messages. More concretely, the Mayor's office set up the Online Hate Crime Hub in 2017 to work with victims to remove hate speech from the internet and prosecute those responsible.' [2273] Thus, with politicians pushing to further reform the system, progress seems to be on its way and will likely surface in the upcoming years as the Internet continues to gain strength through international access.

[2271] Ibid (n 2255) 81.
[2272] Handyside v the United Kingdom [1976] 12 WLUK 53.
[2273] Andrew Wolman, 'Combating Hate Speech at the Local Level: A Comparison of East Asian and European Approaches', (November 18 2019) Nordic Journal of Human Rights, 87-104.

2. Which legislation on the issue of blocking and takedown of internet content does your country have?

2.1 Legal framework on blocking of internet content

The United Kingdom ('UK') does not have one, coherent legislation targeted at regulating the issue of blocking of internet content. A lack of an overarching legal framework was justified by the better efficiency of the voluntary regulation left up to the private sector.[2274] The following allows better flexibility in regulating fast-paced technological developments,[2275] which would be impossible under a generalised approach. It is a usual justification used by the common law countries, which use this approach in other areas of law as well.

Internet Service Providers ('ISPs') act as internet information gatekeepers. As without its services it is impossible to access the web, the online content is overseen by the ISPs self-regulation. In some areas, the legislation has been put in place to complement the self-regulation - for example, the Section 3 of the Terrorism Act 2006, which allows terrorism inciting content to be removed from the public domain[2276]. Especially in cases of defamation and privacy law, courts often order injunctions to prevent access to certain defamatory statements. Compliance solely with the self-regulator's rules is voluntary and bases on the ISPs' collaboration with the UK police as well as other private regulators.[2277] Next paragraphs will describe the role of the most crucial ones and explain their mechanism to blocking the illegal internet content.

2.1.1 Internet Watch Foundation ('IWF')

This industry regulatory body aims to eliminate child sexual abuse imagery online by identifying, assessing and removing illegal imagery.[2278] Its work bases on cooperation with industry partners around the world, including ISPs, to altogether remove and stop such content from being spread further both in the UK and worldwide.[2279] Founded in 1996, it is an independent charity funded by the European Union, the aforementioned online industry (including Amazon Smile) as well as donations from the members of the public.

2274 Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' [2015] 13.

2275 ibid 3.

2276 Terrorism Act 2006, s 3.

2277 Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' [2015] 754

2278 Internet Watch Foundation, 'Our remit and vision' <https://www.iwf.org.uk/what-we-do/why-we-exist/our-remit-and-vision> accessed 15 February 2020.

2279 Ibid.

The IWF relies on other entities not only in regards to its funding. As itself it does not have any special legal permission to intentionally view child sexual abuse imagery during an investigation, it is dependent on the protection given by the memorandum of understanding between Crown Prosecution Service ('CPS') and the Association of Chief Police Officers ('ACPO').[2280] The document also provides protection to IWF's investigators under Section 46 of the Sexual Offences Act 2003 in cases when it is necessary to create 'the photograph or pseudo-photograph for the purposes of the prevention, detection or investigation of crime'.[2281]

One of the crucial projects of the organisation is the creation of the IWF URL list, which contains websites with the illegal images. Conducted by the skilled analysts, the blacklist is updated twice daily to ensure its topicality.[2282] It is then distributed to the industry partners, which block access to all sites included in the document. The exceptions are sites hosted in the UK as those are removed at the source under the Code of Practice for Notice and Takedown (see section 2.2.1)[2283]. Introduction of the list significantly contributed to a decrease in a number of child sexual abuse URLs in the UK from 18% in 1996 to only 0,04% in 2018.[2284]

2.1.2 Counter Terrorism Internet Unit ('CTIRU')

The organisation cooperates with the ISPs to remove unlawful terrorist material content from the web. Unlike the IWF, it works with a specific focus on the UK based materials. The CTIRU has been jointly set up by the Association of Chief Police Officers ('ACPO') in 2010 and relies on the Metropolitan Police's powers to remove the material. Although currently funded from public money, it has been widely suggested that social media companies should contribute to the CTIRU budget.[2285]

Under Section 3 of the Terrorism Act 2006, the police is granted the power to exercise take-down notices.[2286] However, all the procedures are carried out using informal contact between the police and the ISPs thus the Terrorism Act 2006

[2280] Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003.
[2281] Sexual Offences Act 2003, s 46.
[2282] Internet Watch Foundation, 'URL List' <https://www.iwf.org.uk/become-a-member/services-for-members/url-list> accessed 15 February 2020.
[2283] Internet Watch Foundation, 'FC Code of Practice' <https://www.iwf.org.uk/what-we-do/who-we-are/governance/funding-council/fc-code-of-practice> accessed 15 February 2020.
[2284] Internet Watch Foundation, '2018 Annual Report' [2018] 18.
[2285] Home Affairs Select Committee, 'Hate and abuse on social media' https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/60904.htm> accessed 15 February 2020.
[2286] Terrorism Act 2006, s 3.

has actually never been used to block a material encouraging terrorism.[2287] There is no legislative provision under criminal law, which requires a potentially criminally offensive material to be blocked. In practice, however, IPSs usually comply with the police requests to remove illegal material.[2288]

The CTIRU also operates an abroad URLs blacklist, which hosting or distribution in the UK amounts to a criminal offence under the Terrorism Act 2006. So far, it has contributed to the removal of over 300,000 materials encouraging terrorism.[2289]

2.1.3 Website-blocking injunctions under the Copyrights, Designs and Patents Act 1988 ('Copyright Act')

Injunctions require the ISPs to block a third party's material from their domain and it is often used in the areas of copyright, privacy law as well as defamation. Under Section 97A of the Copyright Act, the High Court 'have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright'.[2290] The provision has been used in the *Twentieth Century Fox and others v British Telecommunications plc* case, where the High Court issues an injunction to block access to the Newzbin2 website, which infringed copyrighted material.[2291] The following mechanism allows a degree of flexibility to adjust the wording on a case-by-case basis. There are no limits as for the limits on the type of injunction, which, as in the *Twentieth Century Fox and others*, required the service provider to block access to a whole online service.[2292]

2.1.4 Website-blocking injunctions under the Defamation Act 2013 ('the 2013 Act')

Following the amendments in the UK defamation law by the 2013 Act, secondary publishers are no longer liable for the defamatory materials published on their domain.[2293] Consequently, service providers are no longer liable for defamatory material of this kind, unless the court finds that it is reasonably practicable.[2294] For example, when a defamatory material has been brought to

2287 Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' [2015] 755.
2288 Home Office, 'Hate crime action plan: Challenge it, Report it, Stop it' [2012] 10.
2289 Baroness Williams of Trafford, 'Islam: Tenets – Question' (*TheyWorkForYou*, 7 December 2017) <https://www.theyworkforyou.com/lords/?id=2017-12-07c.1280.3> accessed 15 February.
2290 Copyright, Designs and Patents Act 1998, s 97A.
2291 *Twentieth Century Fox and others v British Telecommunications plc* [2011] EWHC 1981.
2292 ibid 160.
2293 Defamation Act 2013, s 10.
2294 ibid.

the ISPs attention, yet it still contributed to its distribution.[2295] The plaintiff might additionally apply for the order to remove or cease distribution under Section 13 of the 2013 Act.[2296]

2.2 Legal framework on the takedown of internet content

Many of the blocking mechanisms are also used in removing the unlawful material from the internet. Apart from them, it is a common practice of the ISPs to remove the potentially illegal material following a complaint in order to avoid further consequences.[2297] Only unlawful terrorist material (the Terrorism Act 2006[2298]) and defamatory statements (the Defamation Act 2013[2299]) can be subject to statutory 'notice and take-down' procedures. Nevertheless, ISPs usually manage to delete the unlawful material after the receipt of a complaint without intervention from other authorities.[2300] The Electronic Commerce (EC Directive) Regulations 2002 act as an additional incentive to the ISPs to act as mentioned by providing a defence against the liability if the material has been removed or disabled. [2301]

2.2.1 Internet Watch Foundation ('IWF')

Aforementioned Code of Practice for Notice and Takedown regulated the UK-hosted content in terms of child abuse internet content. In 2018, the Code was extended to cover also international companies with the UK-based content.[2302] Notices are issued if the IWF assesses that the material is potentially illegal under one of the following:[2303]

Protection of Children Act 1978

Criminal Justice Act 1988

Sexual Offences Act 2003

Police and Justice Act 2006

Criminal Justice and Immigration Act 2008

2295 *Godfrey v Demon* [1999] Entertainment and Media Law Reports 54.

2296 Defamation Act 2013, s 13.

2297 Emily Laidlaw, 'The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation' [2012] International Journal of Law and Information Technology 20(4) 320.

2298 Find.

2299 Find.

2300 Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' [2012].

2301 The Electronic Commerce (EC Directive) Regulations 2002, regulation 19.

2302 Internet Watch Foundation, 'FC Code of Practice' <https://www.iwf.org.uk/what-we-do/who-we-are/governance/funding-council/fc-code-of-practice> accessed 15 February 2020.

2303 ibid.

Coroners and Justice Act 2009

EC Directive 2000/31/EC, as implemented in England and Wales by the Electronic Commerce (EC Directive) Regulations 2002

Crown Prosecution Service guidelines on indecent photographs of children

The Sexual Offences Definitive Guidelines of the Sentencing Council of England and Wales

If ISP is found to be in breach, the IWF may impose sanctions assessed on the level of seriousness of the breach.[2304] The system is found to be rather effective, with 29,865 postings removed from public access in 2018. [2305]

2.2.2 The Terrorism Act 2006

Identically to the blocking procedure, the Terrorism Act 2006 provides the 'notice and takedown' procedure. Similarly, in practice, the procedure is performed through informal contact between the police and the ISPs.

2.2.3 The Defamation Act 2013 ('the 2013 Act')

Order to remove or cease distribution (Section 13(1))[2306] is permitted for successful claims in defamation cases, where the statement was not published by an operator of a website. Under Section 5(3) an operator is not liable if proven that it was not an author of the statement unless this person cannot be found and the operator failed to remove the statement following the complaint.[2307] In *Tamiz v the United Kingdom*, the ECtHR decided on the liability of Google (as an information society service provider) for defamatory comments posted under a blog post about the claimant. Mr Tamiz' claim based on his rights under Article 8 (Right to Respect for Reputation). It has been confirmed that ISPs are not liable as publishers, yet, to avoid responsibility, they must remove the defamatory statement after the notice had been given.[2308]

2.3 Challenges caused by a lack of specific legislation regulating the issue of blocking and takedown of internet content

With rapid growth of the internet, the UK has been confronted by a magnitude of internet-content-related disputes. The lack of a consistent regulation has become an overwhelming issue and created a gap, which desperately needs filling in. The main issues caused by this legal gap are the following.

[2304] ibid.
[2305] Internet Watch Foundation, '2018 Annual Report' [2018] 39.
[2306] Defamation Act 2013, s 13(1).
[2307] ibid s 5(3).
[2308] *Tamiz v the United Kingdom* App no 3877/14 (ECtHR, 19 September 2017).

2.3.1 A need for independent, accountable and transparent decisions[2309]

A research of the Open Rights Group (ORG) found that there are errors in the online and offline takedown procedures.[2310] Online blocking of internet domains for copyright infringement is not administered properly, resulting in 38% of the blocks being done in error with no current legal basis.[2311] This could be caused by a lack of cooperation between the organisation, for example, the ISPs not notifying the authorities about blocking the domains.[2312] These omissions lead to confusion and consequently, prolongs the length of the whole process of identifying a breach. ORG recommends that one specific legislation is proposed, which would specify the time limits to injunctions and mechanism to ensure efficient cooperation between the organisations.[2313]

2.3.2 Informal censorship by Nominet

Nominet, the Official Registry for .uk Domain Names, currently accepts notice of infringement from eight law enforcement institutions. If accepted, it has the contractual powers to take down illegal internet content. These organisations are not required to have a formal Policy and some of them are not subject to Freedom of Information Act requests. The only requirement is a written request for suspension. There is no independent review of the grounds of suspension nor an independent appeals mechanism. ORG, consequently, suggested adopting Freedom of Information principles as well as a legal framework for domain seizure based on court injunctions.[2314] The IWF does offer an independent appeals system, which could be used as a model for future legal developments.

3. On which ground may internet content be blocked/filtered or taken down/removed in your country?

In the United Kingdom, there are four pivotal grounds for the blocking or removal of internet content. Censorship is entitled under the grounds of defamation, copyright infringement, regulations against incitement to terrorism, and child pornography. This result is achieved through a combination of legislation, judicial action, and voluntary arrangements. The law relies on a

[2309] Open Rights Group, 'UK Internet Regulation – Part 1: Internet Censorship in the UK today' (2018) 1.
[2310] ibid 5.
[2311] ibid.
[2312] ibid 7.
[2313] Open Rights Group, 'UK Internet Regulation – Part 1: Internet Censorship in the UK today' (2018) 1.
[2314] ibid 10.

hybrid approach, which criminalises those who engage with the offending material, and blocking or filtering such material from public view.

Is content which is unlawful in civil law and content which is illegal under criminal law treated differently?

Yes, lawful and unlawful content are treated differently. Lawful content is monitored primarily by ISPs, who have entered into voluntary filtering agreements. These filters include sites promoting pornography, self-harm, or violence, which is a non-exhaustive list. These sites are blocked from users on an opt-out service, where adults are entitled to seek to have this ban lifted from their use of the internet.[2315] This approach has to be contrasted with the legal bases for blocking content on the internet, which can generally be divided into the areas of; defamation, copyright infringement, incitement to terrorism, and child pornography.

Defamation: The UK Ministry of Justice explained that with regards to online defamatory comments, censorship is applied such that,

The purpose of the Defamation Act 2013 is to rebalance the law on defamation to provide more effective protection for freedom of speech while at the same time ensuring that people who have been defamed are able to protect their reputation. In accordance with this aim, Section 5 of the Act creates a new defence to an action for defamation brought against the operator of a website hosting user-generated content where the action is brought in respect of a statement posted on the website.[2316]

However, this legal approach has a corresponding voluntary approach taken by many large websites and ISPs, through which users can report suspicion of defamation, and can ask for the material to be removed.

Copyright Infringement: Copyright is one of the areas which has developed extensive legal oversight for infringement claims. The Copyright, Designs and Patents Act 1988 prohibits file-sharing, and extensive lobbying by the music industry lead to the introduction of the Digital Economy Act 2010.[2317] However,

---

[2315] Jasper Jackson, 'ISPs that restrict porn or block ads could be breaking EU guidelines', (The Guardian, 31st August 2016).
<https://www.theguardian.com/media/2016/aug/31/isps-porn-block-ads-eu-guidelines-sky-bt-talktalk-o2> Accessed 14 February 2020.

[2316] Ministry of Justice, Complaints about defamatory material posted on websites: Guidance on Section 5 of the Defamation Act 2013 and Regulations, (January 2014).

[2317] Bart Cammaerts & Bingchun Meng, 'The government's new Digital Economy Act will do little to prevent file sharing – the music industry must continue to innovate online if it is to survive' LSE GovBlog,
<https://blogs.lse.ac.uk/politicsandpolicy/digital-economy-act-file-sharing-music-industry/> accessed 10 February 2020.

the conventional approach for blocking copyright material is through the courts system, with heavy reliance on the use of court ordered blocking injunctions. Commonly known as 'Section 97As', these orders derive their authority from Section 97A of the 1988 Act, which provides that,

The court may in an action for infringement of copyright having regard to all the circumstances, and in particular to—the flagrancy of the infringement, and any benefit accruing to the defendant by reason of the infringement, award such additional damages as the justice of the case may require.[2318]

In this regard, this censorship area is more heavily entrenched in legalistic procedures than those which rely on the voluntary decisions of major ISPs.

Incitement to Terrorism: In 2010 the Association of Chief Police Officers (ACPO) established the Counter-Terrorism Internet Referral Unit (CTIRU), whose focus is the removal of unlawful terrorist material from the internet.[2319] Once content has been determined unlawful by the CTIRU, there is an onus placed on ISPs to facilitate the removal of this content, on a voluntary basis.

The approach taken by the CTIRU follows legislative definitions of terrorism, 'All referrals are assessed by CTIRU against UK terrorism legislation (Terrorism Act 2000 and 2006). Those that breach this legislation are referred to industry for removal. If industry agrees that it breaches their terms and conditions, they remove it voluntarily.'[2320] The extent of this removal process is impressive, with over 300,000 pieces of illegal terrorist material having been removed since the CTIRU's inception.[2321]

Child Pornography: Child pornography is prohibited under the Protection of Children Act 1978, which made it illegal to take, make, distribute, show, or possess for the intent of showing or distributing an indecent photograph of someone under the age of 18. The case of *R v Bowden* established that, from a digital perspective, saving an indecent image to a computer's hard drive is considered making the image, and can result in up to 10 years imprisonment.[2322]

However, despite the extensive legislative insight, the prohibition on child pornography is self-regulated by ISPs, and this regulation is co-ordinated by the

---

2318 Copyright, Designs and Patents Act 1988, S.97(2).

2319 Brian Chang, 'From Internet Referral Units to International Agreements: Censorship of the Internet by the UK and EU, Columbia Human Rights Law Review, (January 2018), page16.

2320 Sir John Hayes MP, 'Counter-Terrorism: Written Question – 30893', (Parliament.uk. 14 March 2016), <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-03-14/30893/> accessed 04 January 2020.

2321 Open Rights Group, 'UK Internet Regulation Part I: Internet Censorship In The UK Today', page11.

2322 *R v Bowden* [2000] 2 All ER 418

non-profit Internet Watch Foundation. This theme of legislative oversight, with non-judicial regulation at the early stages, continues to be seen here.

4. To which extent is the issue of blocking and taking down internet content self-regulated by the private sector in your country?

4.1 Delegated Powers: Who has the right to censor?

To a certain extent, the UK has safeguards set in place to encourage the blocking and take-down of insensitive and illegal Internet content by private sector agents. With social media taking on such a significant role in every-day life on the Internet, the UK has recently noted that there is a serious need to hold these platforms accountable for the content that is spread and shared on their respective pages. In the upcoming years Ofcom – a content regulator in the UK – is seeking to 'make social media companies such as Facebook (FB.O) and Twitter (TWTR.N) responsible for harmful content on their platforms.' [2323]

In fact, there have recently been a lot of discussions in the UK about setting more online safety laws that maintain order and warrant accountability of online communications in order to promote a safe space for all. Under such proposals, the government is seeking to enforce laws by which 'social media platforms will have to remove illegal content quickly [or otherwise face big fines] and minimise the risk of it appearing at all.' [2324] Nevertheless, the UK Crown Prosecution Services have 'admitted that social media was raising "difficult issues of principle" and these had to be "confronted not only by prosecutor but also by other including the police, the courts and service providers" [however, not] all statements, even offensive remarks, need to face criminal prosecution.'[2325]

As of today, Ofcom is known in the UK for having delegated powers under the Communications Act of 2003. [2326] While Ofcom is set in place to protect the freedom of expression, it is also responsible for content regulation and, to some degree, censorship. Ofcom has 'statutory backstop powers in relation to PRS. It is responsible for approving the code and, under section 121 of the Communications Act 2003, for setting the conditions under which PRS providers can operate.' [2327] Furthermore, recent initiatives have also introduced

---

[2323] Paul Sandle, 'UK to make social media platforms responsible for harmful content – BBC', *Thomas Reuters*, Technology News, (February 12 2020).

[2324] ibid.

[2325] Paul Sandle, 'UK to make social media platforms responsible for harmful content – BBC', *Thomas Reuters*, Technology News, (February 12 2020). 118.

[2326] Communications Act 2003, c.21

[2327] Christopher T. Marsden, *Internet Co-Regulation*, Cambridge University Press, (2011), 134.

Internet filtering through private Internet Service Provider (ISP) censorship. IPSs are not 'only responsible for content when it has been given notice of its potential harmful or illegal nature, at which point it may take down such content prior to investigating the complaint – the so-called "Notice and Take Down" (NTD) regime under ECD.' [2328] Nonetheless, there have been contestations to such safeguards 'in light of fundamental procedural human rights guarantees of freedom of expression. This includes the ability to challenge decisions to filter/block content and (not) to give notice to affected users.' [2329]

4.2 Publisher's Liability & Data Protection

As previously stated, Britain is seeking to increasingly establish liability on publishers in order to encourage more careful consideration of the content and data published and spread online. In April of 2013 Google 'faced legal action from the data-protection authorities from six different states (Germany, France, the Netherlands, Spain, Italy and Britain) for a failure to change its privacy policy after concerns about the harmonisation of privacy policies between different Google services.'[2330] More particularly, the UK established on this matter that 'Google can be held liable for comments published on Blogger, its online blogging platform, unless it reacts immediately to a complaint.[2331]

However, this concept of publisher's liability and data protection has sparked much polarised discussions over its threat on freedom of speech, especially in regards to content that is not objectively illegal, per say. In such, it is understood that this system encourages platforms to 'delete even potentially defamatory material immediately after having been notified even if the material is not illegal at all. According to Article 19, this creates a "worrying chilling effect on freedom of expression as intermediaries might censor perfectly legitimate speech."' [2332] It becomes clear that States are faced with a very difficult challenge of finding a balance between the concepts of freedom of expression and civil protection.

The Internet has unquestionably made it very easy to cross that line and infringe on individuals' fundamental human rights, whether it be freedom of expression, the freedom of thought and consciousness or the right to be protected from discrimination. In inviting external agents like Ofcom, ISPs and the Internet Watch Foundation, the UK has brought into questions its intention to preserve the freedom of expression through what has seemed to many like an increased

[2328] ibid, 164.
[2329] Christopher T. Marsden, *Internet Co-Regulation*, Cambridge University Press, (2011), 143.
[2330] ibid (n 2255) 120.
[2331] ibid (n 2255) 123.
[2332] Christopher T. Marsden, *Internet Co-Regulation*, Cambridge University Press, (2011), 123.

notion of censorship and/or monitorisation of online content – which for some is positively received but for others is a dishonourable overstep.

5. Does your country apply specific legislation on the "right to be forgotten" or the "right to delete"?

In the United Kingdom the Data Protection Act 2018 has been introduced bringing into force the EU's GDPR standards. This will therefore, prevail after the implementation of Brexit. The legislation ensures that organisations take into account the risks of processing personal data and that they put into force ways to mitigate the risks.

Numerous cases have been brought against Google, who after the landmark case of *Google Spain*[2333], has consequently put into place an online form where anyone can make a direct request to exercise 'their Right to be Forgotten'. In 2018 two cases were brought in the United Kingdom against Google[2334], here one of the key issues was the balancing of this right against freedom of expression and the public interest. This is the case because 'the Right to be Forgotten' is not an absolute right. The ruling has established that the personal information shall be seen to be 'out of date, irrelevant and of no sufficient legitimate interest to users of Google Search'[2335], in order to justify its removal.

The way this Right might be implemented by the UK courts post-Brexit might differ, as the decisions from the European Court of Justice will not have to be followed, but a very similar standard will stay in place. Moreover, it seems like the United Kingdom has intentions not only to carry on implementing strict legal measures on search engines but also on social media platforms.[2336]

6. How does your country regulate the liability of internet intermediaries?

6.1 Intermediaries as regulatory power

Internet is an international information communication network that allows multiple computers to connect peer-to-peer by following a spectacular method.

2333 Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez (Case C-131/12).

2334 (1) NT1 & (2) NT2 v Google LLC [2018] EWHC 799 .

2335 ibid, para [223].

2336 Sandle.P, *Britain to make social media platforms responsible for harmful content,* <<https://in.reuters.com/article/britain-tech-regulation/uk-to-make-social-media-platforms-responsible-for-harmful-content-bbc-idINKBN2060RC >> (Accessed on the 12th of February 2000)

It is the network of Internet networks.[2337] Mainly since the beginning of the 1990s, it has spread rapidly. It has become an unlimited mass media. Today, millions of people are connected to the internet and embrace it as part of their life. The internet has an autonomous structure. Each one is made up of independently controlled, supervised networks. When assessed in this sense, it is a structure that is controlled in an individual sense but does not have management and denial in a global scale. This free environment has created opportunities for people in many different areas, as well as a place where a number of crimes can be handled easily. Parallel to the increase in Internet usage, publications with illegal content on the internet has increased significantly. Despite these problems, the free and independent structure of the internet is an essential factor in the spread of the internet. There are many actors affecting internet infrastructure, and each of them has different duties. Although some experts[2338] in the governance of internet may think that states and case law substantially govern this area, internet service providers have significant influence and essential duties through, e.g. notice-takedown and blocking for enforcement of rules on internet users. In practice, internet reaches users by these internet service providers, and they are the main actors of enforcement in this infrastructure. Daniel Seng expressed ISP's integration to the enforcement as legal guardians rather than the subject.[2339] The present system of enforcement of rules on internet users depends (majorly) on the expectations and duties performed by these service providers. Google, Yahoo and Facebook design and enforce rules through their policies on internet users within the scope of contract law (terms of service and terms of use). Assessment of Internet Service Providers' action and duties imposed by case law or governments is critical to show their significant role in the enforcement of rules on internet users.

6.2 Information Society Service Provider Regime

The ECD has established a definition of an information society service provider which envisions boundaries broader than the known service provider concept. This definition, including Internet service providers, is organised in the title of section 4 as intermediary service providers. These 'Service providers' are defined as 'any natural or legal person providing an information society service' (Article 2(b)), which is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'. Article

[2337] A. Mary, 'Internet Copyright Infringement Liability: Is an Online Access Provider More Like A Landlord Or A Dance Hall Operator' (1997) 27 Golden Gate University Law Review.

[2338] A. Mary, 'Internet Copyright Infringement Liability: Is an Online Access Provider More Like A Landlord Or A Dance Hall Operator' (1997) 27 Golden Gate University Law Review.

[2339] Seng D. 'Comparative Analysis Of National Approaches Of The Liability Of The Internet Intermediaries' Wipo (22 June 2011)

2(a) defining 'information society services' by reference to the definition of 'services' in Article 1(2) of Directive 98/34/EC,[2340] as amended by Directive 98/48/EC.[2341]

This broad concept includes not only traditional internet service providers (access providers) but also contains wide range of players involved in selling goods or services online (e-commerce websites such as Alibaba, Amazon; serving as a commercial search tool (e.g. Google and Yahoo); providing information for revenue (e.g. Westlaw); and network service access companies and telecommunication companies.

In order to determine the effect of Internet Service Providers and law on users, the definition and legal position of service providers should be examined first. Internet Service Providers are real or legal entities that provide access to users internally or mediate the provision of electronic services to users. By using the internet in a practical and useful way, we can identify each real or legal person as a user who will take part in an information society. ISP's responsibilities are determined based on the nature of the service they perform. The responsibilities of the ISP, which prepares the content with the Internet service provider and the access service, providing only the Internet access service (mere conduit), will be evaluated differently.

While Internet Access Providers offer only fundamental communications other than web hosting or other (services such as access, information storage etc.), Internet Service Providers (ISPs) may supply 'some additional service which facilitates a transaction between end-users, e.g. identifying one of the parties, providing search facilities etc.' The transformation of providers to a monopoly for web search, e-mail, web storage and access blurred the line between internet service providers and internet access providers.

The term and concept of 'intermediary' are not referring to an objective reality ascertainable purely by examining facts, but an elastic concept used by the intermediaries themselves and other interested parties to resist or assert regulatory burdens. That resistance or assertion is never justified simply by claiming or denying the status of an 'intermediary'. The political or policy dimension of identifying an online actor as an intermediary also shines through in the fact that even if an actor is identified as an intermediary for some legal purposes, and thus subject to some duties in respect of the communication, does not mean that that same status would also be granted in another area of law. For example, just because Google has minimal liability for defamatory content on its

[2340] Directive 98/34/Ec Article 2(A).
[2341] Art 1(2) Of Directive 98/34/Ec, As Amended By Directive 98/48/Ec.

search results under English law does not mean that it is similarly immune under data protection law, so intermediary liability cannot be pinned down simply by reference to what an online actor does in the communication chain but is a malleable concept responsive to economic and political conflicts of the time.

6.3 Search Engines and Social Platforms (e.g. Google, Yahoo and Facebook)

Google, Yahoo and Facebook are internet service providers offering a wide array of utilities such as online advertising technologies, search engines, cloud computing, software, and hardware. It is possible to draw a legal picture for these intermediaries concerning Article 12 Electronic Commerce Directive;[2342] section 5, Defamation Act 2013;[2343] section 512(a) DMCA Article 11 Enforcement Directive;[2344] Article 8(3) Information Society Directive[2345] for Mere facilitator/tool/device role which does not (provide) liability, section 1(1) Defamation Act 1996 (publisher/distributor); Article 13, 14 Electronic Commerce Directive;[2346] section 512(b),(c),(d) DMCA[2347] which offers Secondary/contributory liability (take-down duty upon notification and no monitoring duty) for intermediary role,' e.g. section 1(2) Defamation Act 1996 (author, editor, publisher,) which offers primary liability.

From Google's, Yahoo's and Facebook's perspective, different types of information society service providers perform different functions. They also have different technical architectures. For example, internet access providers (traditional type ISPs such as Vodafone, and Talk Talk) connect a user's device, whether it is a laptop, mobile phone or anything else, to the network of networks known as the internet. It is a web hosting provider that allows to connect to your website and connect to the internet. Search engines make up a portion of the World Wide Web. Search engines are an essential go-to between websites and internet users (e.g. Google 67.5 per market share in US Yandex dominates in Russia with 62 per cent market share[2348] and Yahoo.)[2349] Social networks connect individual internet users by allowing them to exchange text, photos, videos (e.g. Facebook and Twitter).[2350]

2342 Article 12 Of Electronic Commerce Directive.
2343 Article 5 Article 12 Of Defamation Act 2013.
2344 Article 12 Of Electronic Commerce Directive.
2345 S.5 Article 12 Of Defamation Act 2013.
2346 Article 11 Of DMCA S.512(A).
2347 Art 8(3) Of Information Society Directive.
2348 Defamation Act 1996 S.1(1).
2349 Electronic Commerce Directive Article 13, 14.
2350 S.512(B),(C),(D) Of DMCA.

6.4 Company Policies and Legal Requirements

As a member of the Global Network Initiative, Google promised to interpret content removal requests from competent authorities as narrowly as possible and to appeal incompatible requests for related laws.[2351] Google publishes information about government and specific requests for content removal and filtering and the process of responding to them. The company's 'Transparency Report' points out that it challenges or refuses to comply with a significant percentage of government requests across the world.[2352] When Google comply with a government request to restrict content in a jurisdiction, the content is restricted from view only in the jurisdiction where the request was made, unless the content violates the company's terms of service.[2353] (Just as it is a 'forgotten' case, in European court decisions that will apply to the entire European Union, Google has interpreted this commitment to apply to its online properties in the EU.) Apart from this, illegal child pornography is a content category that removes government requests voluntarily and proactively from search results.[2354]

Another search engine Yandex, in the case of enforcement of rules, clearly expressed internet service providers' position and the power they have; Even for a search engine who has no other prohibition policy (the only google have in search engines) other than law do not accept the extreme requests. For example, several Russian laws passed between 2012 and 2014 empower the government's executive branch to blacklist 'extremist' content, content deemed harmful to

---

2351 Smith C. By The Numbers: 40 Amazing Google Stats And Facts. Digital Marketing Ramblings. Http://Expandedramblings.Com/Index.Php/By-The-Numbers-A-Gigantic-List-Of-Google-Stats-Andfacts. Accessed Ben Rooney. Microsoft, Google Join To Battle Child Porn. Wall Street Journal. 18 November 2013. Http://Online.Wsj.Com/News/Articles/Sb40001424052702304439804579205874211710440

2352 See Google Transparency Report. Requests To Remove Content. From Government. Summary Of All Requests. Https://Www.Google.Com/Transparencyreport/Removals/Government/ R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role Of Internet Intermediaries. Other Publications From The Center For Global Communication Studies.

2353 See Google Transparency Report. Turkey. Http://Www.Google.Com/Transparencyreport/Removals/ Government/Tr/ For Example In The January-June 2013 Reporting Period: "We Received 1,126 Requests From Government Agencies To Remove A Total Of 1,345 Items From Blogger, Google+, And Web Search That The Agencies Claimed Were In Violation Of Law 5651. We Removed 188 Items That Violated Our Product Policies." Also See: Jeff Landale. Google Transparency Report Sheds Light On Internet Threats. 6 December 2012. Https://Www.Accessnow.Org/Blog/2012/12/06/Googletransparency-Report-Sheds-Light-On-Internet-Threats Accessed R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role Of Internet Intermediaries. Other Publications From The Center For Global Communication Studies.

2354 Ben Rooney. Microsoft, Google Join To Battle Child Porn. Wall Street Journal. 18 November 2013. Http://Online.Wsj.Com/News/Articles/Sb40001424052702304439804579205874211710440 (.) Global Network Initiative Implementation Guidelines. Https://Globalnetworkinitiative.Org/Implementationguidelines/Index.Php 107 Demands To Remove Or Filter Content.

minors, and copyright-infringing content among other content without requiring a court order.

Despite being requested, Yandex executives have indicated that there is no blocking or filtering by Yandex in the search results and other services. Only if the contents of the web site are deleted, the contents disappear.[2355]

Outside of the jurisdictions, services with large user base such as Facebook may act to restrict content in response to government requests. Photos of children's sexual abuse are the only type of content that Facebook proactively tracks or illegally pulls out without a government request, court decision or copyright take-down notice. Facebook was the first company to use Microsoft's PhotoDNA to detect 99.7% of children's sexual abuse photos in 2011. Facebook is open to policymakers around the world to respond to all restriction requests and questions coming from governmental authorities.[2356] Facebook may use an authoritative restraint mechanism if its content violates the service terms of the company and is not illegal in the United States: the content is limited to users in countries that are found to be infringing only on local laws and governments, where specific legal requirements apply.[2357] In this way, users may access content in other areas.

6.5 Legal context in UK

There is no legal framework specific to the internet in the UK. As a result, the country is based on general laws on removing or blocking illegal content online. The UK encourages voluntary actions to solve these problems in cooperation with the private sector. The removal and blocking of online content in the UK are mostly done through specific regulations: regulatory agencies, either taking the form of rules for the use policies of intermediaries with national authorities, copyright owners and individuals.[2358]

IWF, as a regulatory body cooperates with intermediaries to prevent child sexual abuse, publishes good practice guidance on blocking. IWF also publishes a

---

[2355] See Google Transparency Report. Requests To Remove Content. From Government. Summary Of All Requests. Https://Www.Google.Com/Transparencyreport/Removals/Government/ R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role Of Internet Intermediaries. Other Publications From The Center For Global Communication Studies.

[2356] R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role Of Internet Intermediaries. Other Publications From The Center For Global Communication Studies.

[2357] Https://Govtrequests.Facebook.Com/About Twitter Restricts Content On A Reactive Basis And On Receipt Of 'A Valid And Properly Scoped Request From An Authorized Entity'. Twitter. Help Center. Country Withheld Content. Https://Support.Twitter.Com/Articles/20169222-Country-Withheld-Content.

[2358] Council of Europe, "Etude Comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, 2015", *op.cit., page* 13.

blacklist hosted abroad and notifies Internet Service Providers who must block them.[2359] Parties may apply for a reassessment of these considerations. This guidance is essential to minimise over-blocking therefore helps protecting individual rights such as freedom of speech and right to information/access.[2360]

In addition to this, UK legal system has a specific legal approach on some specific issues such as terrorist contents defamation and copyright breaches. Service policies or judiciary feature in blocking orders depending on content type. For example, the Terrorist Act 2006 gives police services power to issue blocking order. However, cooperation with intermediaries is a must in practice.

Court issues blocking injunctions to access certain sites only in the case of a defamation or copyright breaches. The 1988 Copyright, Designs and Patents Act authorises the Supreme Court to take such measures against an intermediary with 'real knowledge' that the content in question violates the copyright law.[2361] Statutory provisions for the notice and take-down process is only possible for defamation and contents related to terror; however, in practice, intermediaries cooperates for other areas to avoid possible liability. [2362]

6.6 Regulatory Duty in The Legal Context

This part is to explain the regulatory role of these intermediaries and duties performed by them in the present system and to show the importance/role of Internet Service Providers (intermediaries) for the enforcement of rules on internet users.

Influential media industry members have an aggressive strategy to maintain their propriety rights. Legal framework given narrower copyright infringement immunity than other legal areas and this strategy creates a complicated and

---

[2359] Council of Europe, "Etude Comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet", *op.cit., page* 17.

[2360] https://repository.gchumanrights.org/bitstream/handle/20.500.11825/594/Timmermans.pdf?sequence=1&isAllowed=y

[2361] See Google Transparency Report. Turkey. Http://Www.Google.Com/Transparencyreport/Removals/ Government/Tr/ For Example In The January-June 2013 Reporting Period: "We Received 1,126 Requests From Government Agencies To Remove A Total Of 1,345 Items From Blogger, Google+, And Web Search That The Agencies Claimed Were In Violation Of Law 5651. We Removed 188 Items That Violated Our Product Policies." Also See: Jeff Landale. Google Transparency Report Sheds Light On Internet Threats. 6 December 2012. Https://Www.Accessnow.Org/Blog/2012/12/06/Googletransparency-Report-Sheds-Light-On-Internet-Threats. R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role Of Internet Intermediaries. Other Publications From The Center For Global Communication Studies.

[2362] Swiss Institue of Comparative Law, *op.cit.*, page 756.Section 97A of the Copyright, Designs and Patents Act 1988. Swiss Institute of Comparative Law, *op.cit.*, pp. 758-760. *Ibid., page* 753. R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role Of Internet Intermediaries. Other Publications From The Center For Global Communication Studies.

critical relationship for industry, online actors (ISPs) and internet users. Although copyright law is a vital area for internet service provider involvements, the regulatory role of these service providers shows its effect on many areas (such as data protection and defamation)

If we consider that search engines and social platforms are extraordinary online players, the number of lawsuits and regulations is expected with their financial capacity. However, it should be remembered that the following discussion (other than on competition) focuses on the legal contexts in which the search engine is not primarily wrongdoer but is included as another regulatory force in the legal process.

7. Based on your analysis, how do you believe that legislation regarding online content blocking and take-down, liability of internet intermediaries and the right to be forgotten will develop in your country over the next five years?

7.1 Notice-and-takedown Concept

While other types of internet service provider involvements are not on the ground of wrongdoing. Notice and take-down duty have a specific character which can be expressed as 'shaped by regulations and case law and reshapes the enforcement'.[2363] Uta Kohl stated this role as "quasi-regulators (within private-public partnerships) as opposed to being part of 'the regulated'".[2364]

Take-down duty and frame (associated by US Digital Millennium Copyright Act for US, Electronic Commerce Directive) for the UK for, however, case law and new regulations have an ever-increasing influence) defined as the key concept for enforcement of copyright. Information giants showed their intention to have immunity for secondary liability, 'safe harbour' and created their notice and take down the system as a part of limited liability regime for online intermediaries. While that explanation considered, the concept might seem as governance of regulations and case law.

However, the practice underlines the regulatory power of these online intermediaries but these information giants built a request respond system teams

[2363] M. Chris Lecture Document Dated 12.10.2017 (Week 5 Of 2017-2018) Https://Govtrequests.Facebook.Com/About Twitter Restricts Content On A Reactive Basis And On Receipt Of 'A Valid And Properly Scoped Request From An Authorized Entity'. Twitter. Help Center. Country Withheld Content. Https://Support.Twitter.Com/Articles/20169222-Country-Withheld-Content.

[2364] M. Chris Lecture Document Dated 12.10.2017 (Week 5 Of 2017-2018).

consisted of thousands of people and trained them in the light of company strategies which cannot be monitored entirely (Google has its prohibitions in Google terms of service and Google privacy policy).[2365] The only immunity borderline is 'failing to respond to the notice expeditiously' in case of being noticed about wrongdoing.[2366] For example, Google, Facebook and Yahoo created their terms of use in compliance with Regulations designing the liability regime for online intermediaries 17 US Code section 512 - Limitations on liability relating to material online. These US-based regulation designs the immunity regime by the article expressing that 'The limitations on liability established by this section shall apply to a service provider only if the service provider, (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers'. As a result of the regulation mentioned above Google created intellectual rights policy including repeated infringers as ('We respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the US Digital Millennium Copyright Act'. and "We provide information to help copyright holders manage their intellectual property online. 'If you think somebody is violating your copyrights and want to notify us, you can find information about submitting notices and Google's policy about responding to notices in our Help Centre.') this case is going to be discussed in blocking part in a broader context. The giant internet service providers design their policy depending on their immunity-based strategy.

Google has a long history of responding to rights holders" take-down requests by removing the content from search results. Between the dates of 1 July 2011 and 31 December 2011, Google published that 97% of request concluded by removing the content from search results.[2367] According to the transparency reports dated 6 January 2018, that high ratings fluctuating even for big media companies in lower rates. These change mostly the consequence of the system providing counter-request notice and concerns about the possibility of using notices to harm rivals. Similarly, Facebook stated copyright request report action rate as 68.43% between January and June 2017 for 224,464 requests. These rates

[2365] Google Privacy Policy.

[2366] Ibid.

[2367] Google *Transparency Report Faq* <Http://Www.Google.Com/Transparencyreport/Removals/Copyright/Faq/> Accessed, For The Period Between July And December 2011, Google States That It 'Removed 97% Of Search Results Specified In Requests'.

not only show the importance of these giants' regulatory role but also shows these companies engage with community expectations.

In European Union, although there were notice and take-down duty in areas such as data protection and defamation before the Electronic Commerce Directive (ECD), limited liability (immunity) system associated with ECD which only regulates immunities from existing liability. In Richardson v Facebook (2015)[2368], Mr Justice Warby dismissed the claimant's appeal claim against Facebook UK (not Facebook Inc.) for defamation and breach of Article 8 ECHR for comments on a fake profile page created by a user of the website. Warby expressed the reason for dismissing defamation claim as Facebook UK had 'any form of control over any aspect of the content of the Facebook Service' even assuming that allegation is not the case, there was no 'proper basis for the attribution of responsibility for publication based on Byrne v Deane principles.' Justice Warby found that power to take an action (upon being informed) is the primary basis of publisher in common law. The judge mentioned this landmark case shaping the liability of natural and legal person controlling the notice board and has the acting power to remove wrongful content (posting) posted by a third party to show defendants were responsible.[2369] Most significantly, The *Byrne v Deane* (1937) case concerned the liability of a golf club for the anonymous defamatory posting on its notice board after it became aware of it; the court recognised responsibility for the publication based on the fact that 'they were entitled as proprietors to remove the trespassing article from the walls. The importance of the case for this essay part is not about the dismissal of the case based on the territorial issue, and it is about the case mentioned *Byrne v Deane* (1937) showing the historical process of the duty on service providers in case law. Thus, intermediaries are being involved in the regulatory process based on practical considerations: they are obliged to take-down material, if and because they can. These intermediaries have a substantial capacity to regulate and control users on internet. Although using them through legislation and case law is a choice, other ways of using them (by cooperation) must be considered. For example, Google has its company policy (as mentioned above) not only includes law rules of government and state laws but also have its specific policies which control its environment quickly and reasonably. Although the take-down policy is mostly a part of the immunity-based strategy for the company (Google), Google uses this system for its own extra prohibition rules.[2370]

[2368] Richardson V Facebook (2015) [2015] Ewhc 3154 (Qb).
[2369] Byrne V Deane (1937 1 Kb 818).
[2370] Smith C. By The Numbers: 40 Amazing Google Stats And Facts. Digital Marketing Ramblings.

Yet, as noted above, the status of an intermediary for one legal purpose is by no means a once-and-for-all decision. For data protection, the CJEU held that Google was indeed under an obligation to de-index certain search results to a person name search. For this reason, considered a significant case for primary liability.

7.2 Blocking

LICRA vs YAHOO is one of the most important cases that show how effective local courts can be in terms of enforcing rules on internet users and how local powers can use information giants effectively. It also sheds light on measures taken by Yahoo regarding its terms of service after that territorial conflict.

In France, in the Jewish Student Association and anti-racist LICRA's application on the Yahoo auction site for a collection of Nazi memorabilia, the French court found that Yahoo could establish that 90% of user IPs connected from France. Hence the court has decided that the users connected from France should take measures to prevent access to prohibited content; otherwise criminal sanctions should be imposed, and the proceeds of the Yahoo office in France be confiscated. On this incident in 2000, Yahoo blocked the sale of Nazi memorabilia from auction sites in January 2001.

Yahoo then sought a declaratory judgment from the District Court of California precluding enforcement in the US of a French court order intended to regulate the content of the company's US website. LICRA appealed to the US Court of Appeals (9th Circuit), and the Court of Appeals reversed the judgment of the District Court (it is to be noted that the majority of the Court of Appeal held that the District Court did have proper personal jurisdiction over LICRA, but the judges did not all reach the decision to reverse the decision of the District Court for the same reasons).

The E-Commerce Directive purports to provide a greater level of certainty amongst the European Union's member states through the 'country of origin' principle. Under the E-Commerce Directive, a provider of 'information society services' (for these purposes, anyone who conducts business electronically) with the centre of its business activities in one-member state will be governed by the laws of that member state notwithstanding the fact the provider's services may be accessed by residents of other member states with differing laws. However, this harmonising principle does not apply to all arrangements. For example, the

Http://Expandedramblings.Com/Index.Php/By-The-Numbers-A-Gigantic-List-Of-Google-Stats-Andfacts.

E-Commerce Directive excludes from its ambit national laws governing contractual obligations concerning terms of services and data policy.

As a result, EU consumers can rely on suppliers to enforce their countries' laws on the quality and quantity of goods, insufficient contractual conditions and other consumer customs regulations.

In light of the fact that certain jurisdictions wish to adopt a 'long-arm' approach, service providers (Yahoo in that case) are set up their sites and draft their terms and conditions so that it is abundantly clear that they intend to target and contract only under certain circumstances. Quite apart from sanctions that may be imposed on these providers, and of course, negative publicity and loss of sales from customers in such jurisdictions, the immediate practical concern for suppliers are that they may own assets in these jurisdictions that may be used to satisfy judgments awarded against them. Yahoo and other internet service providers are in an effort to evade being forced to stop an activity or the liabilities by disclaimers in their terms of service;[2371] however, these disclaimers will be in the hands of courts.

In the light of Yahoo's reaction, this case can be expressed as a win for national case law, but also the course of events underlines the importance of internet service provider's duty.

The rationale behind the blocking concept is to stop illegal activities similar to the notice-and-takedown process. Blocking measure can be seen in the form of website blocking, or directly user blocking. Blocking duty of internet service providers (e.g. Facebook, Google, Yahoo) is commonly seen as blocking the user. The main structure of copyright policies designed by the concept (procedure) commonly called 'graduated response', mostly expressed as a three-strike rule. The aim was to reduce infringing activities on internet. Although this policy was adopted in many countries as a part of their law, in some countries it is carried on voluntarily (e.g. United States). In the UK, this policy is regulated by Digital Economy Act 2010.[2372] When the three big internet service providers (Yahoo, Google and Facebook) considered, Yahoo adopted this concept to their policy as 'terminate accounts of repeat infringers according to the process set out in the US Digital Millennium Copyright Act'. Yahoo respects the intellectual property of others, and we ask our users to do the same. Yahoo may, in appropriate circumstances and at its discretion, disable or terminate the accounts of users who may be repeat infringers'. Google adopted the same concept as 'We

[2371] Facebook Terms Of Service Https://Www.Facebook.Com/Terms Accessed Yahoo Terms Of Service Https://Policies.Yahoo.Com/Us/En/Yahoo/Terms Accessed.
[2372] Digital Economy Act 2010.

respond to notices of alleged copyright infringement and terminate accounts of repeat infringers according to the process set out in the US Digital Millennium Copyright Act, and Facebook adopted as 'If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate'.

Luridly, blocking concept is widely used by authoritarian governments. While countries have developed legal systems respect human rights and try to balance blocking injunctions and human rights (e.g. freedom of expression), some authoritarian regimes use these injunctions to control environment through intermediary service providers or access providers.

7.3 The Dominance of Internet Service Provider

Internet infrastructure is the main reason for the service provider's essential role. Even in the cases can be expressed as shaped by regulation and shaping regulation situation enforcement of rules on internet users is not possible because of the nature of internet infrastructure. A search engine can reject requests by governments and case law (Yandex and Google). While Governments and Case law supporters enjoy little wins in some cases, they should not forget that the way to enforce this small trophy through these internet service providers.

Even information service providers revise their policies such as terms of service and privacy policies we should not forget that these revisions are being made for company strategies and no power may force internet service providers (which are active business entities)

This paper addressed the significance and importance of internet service providers through its duties and role related to case law, regulations and company policies. The government will need to expand the role of courts can issue blocking injunctions. Police services will be more actively engaging in blocking to fasten the process (instead of courts) .

Abovementioned materials show the dominance of intermediaries in practice. Even if the regulators may well be trying to tighten liability regimes for intermediaries, Self-regulation will be the mainstream via their terms and services and are already able to reflect their bias on business interests.

8. Has your country reached an adequate balance between allowing freedom of expression online and protecting against hate speech in online environment? If not, what needs to be done to reach such balance?

Hate speech is one of the main issues what the legislation has to face nowadays. Everyone agrees hate speech should not be the case, but still it is an existing problem both in our everyday life, and in the internet era. The hate can be because of someone's race, someone's age or even because they live in an other country. And it is only the start of the list, and the reasons are just going and going on.

Although there are some new duties imposed on internet service providers such as monitoring and identification of wrongdoers, these two other concepts regulated in rigid regimes relatively, these four concepts are essential for the enforcement of rules on internet users. Although some of them have supporting roles, others impose proactive duties on internet service providers.

With the emergence of the internet, the necessity of applying the existing rules of law to a new space of cyberspace emerged; on the other hand, new and unprecedented rights violations unique to the internet have begun to be seen. The internet is a field that is still unknown to governments and is trying to be understood. The shortcomings of this issue as well as the structure of the internet increase the dominance of internet service providers seriously. It is a matter of the fact that the people in the real-life also obey the rule rules and the rule rules on the internet. Of course, one of the most critical questions that come to mind here is whether case law and legislations are more critical in the case of enforcement of rules, or service providers have a more critical role. In this case, the impact of case law, state legislation, and internet service providers' rules on Internet users have been assessed in the context of regulatory roles of Internet service providers. As a result, it has been revealed that internet service providers are the most powerful actors in applying the rules on users. Even though the case law and the regulations are influential both on the service providers and on the users, in practice, actions of the service providers are more important based on the exercise of enforcement in internet infrastructure.

Enforcement of rules on internet users is not possible without service providers to support because of the internet infrastructure nature. A service provider can reject requests by governments and case law under certain circumstances (According to Google transparency report unless the content is violating Google' terms of service, restrictions upon request only be forced in the

jurisdiction). While Governments and Case law supporters enjoy little wins in some cases, they should not forget that the way to enjoy this small trophy through these internet service providers. Although information service providers revise their policies such as terms of service and privacy policies, we should not forget that these revisions are being made for company strategies and this commercial perspective could not affect service providers' dominance on user enforcement.

With respect to the abovementioned cases, regulation, the internet service provider actions and the internet infrastructure, internet service providers have a great influence and have a massive duty for enforcement of rules on internet users.

One way how the UK is fighting against hate speech is blocking and delating. However, that is just only the starting point. The legislation cannot change the population's view, but the legislation should provide more protection against hates peach, maybe even to criminalise hate speech.

9. Has your country reached an adequate balance between allowing freedom of expression online and protecting other rights? If not, what needs to be done to reach such balance?

The concept of content regulations has faced much criticism as it imposes on the fundamental human right of freedom of expression. Some feel it to be a gateway to censorship through over-blocking. Service providers are given the right to moderate and filter content with the purpose of providing a safer space online, such as Ofcom, ISPs as well as the non-profit organisation Internet Watch Foundation (IWF). Through their services, much like the others, IWF seeks to make an impact on an international scale through moderation and censorship of content that has to do with '[c]hild sexual abuse content hosted anywhere in the word [and] non-photographic child sexual abuse images hosted in the UK.' [2373]

Through the monitorisation of this agency 'most UK residents can no longer edit the volunteer-written encyclopaedia, nor can they access an article in it'. [2374] Through the blocking of URLs and censorship of content, some believe the use of this power to be excessive, and 'while the overall goal of IWF and similar hotlines is important, the practical denial of procedural protections of freedom

[2373] Internet Watch Foundation, 'What we do', (2020) https://www.iwf.org.uk/what-we-do
[2374] Ibid (n 2255) 119.

of expression can lead to serious negative consequences.'[2375] Therefore, the government – along with these private organisations – ought to proceed in an adequate fashion in order to avoid endangering the fundamental human right of freedom of speech – or the perception of it.

Based on the current legislation, the United Kingdom is following an overprotecting policy, which might reduce expression rights.

10. How do you rank the access to freedom of expression online in your country?

The United Kingdom currently sits in 33rd place worldwide in the 2019 World Press Freedom Index.[2376] Although out of 180 countries included in a ranking, the 33rd place does not seem to be tragic, the UK is way behind some other Western-European countries. With the legal uncertainty regarding Brexit and a lack of unified approaches in the cases of illegal material takedown and blocking, the country is facing an unknown future. For this reason, we have ranked the access to freedom of expression online in the United Kingdom at 3 points out of 5.

10.1 Advantages of the current system

In a joint statement of the Global Partners Digital, Index on Censorship and Open Rights Group, it was held that the existing legislation does protect the British people from harmful content. Although it must be noted, the legislation is not perfect.[2377] As described in 2.1.1, the IWF has made incredible progress in fighting against presence of child abuse online. By cooperating with the public, CTIRU has successfully managed to arrest several individuals for terrorism offences.[2378]

We must note the UK government is not ignoring the issue. Recently, there has been a number of developments aimed to improve Freedom of Expression in the United Kingdom. Last April the Online Harms White Paper was published,

---

[2375] Ibid (n 2255) 120.

[2376] Reporters Without Borders, '2019 World Press Freedom Index' <https://rsf.org/en/ranking> accessed 16 February 2020.

[2377] Index on Censorship, 'Adopt a 'human rights by design' approach towards regulating online content, say civil society groups' (*Index*, 16 October 2016) <https://www.indexoncensorship.org/2018/10/adopt-a-human-rights-by-design-approach-towards-regulating-online-content-say-civil-society-groups/> accessed 16 February 2020.

[2378] Counter Terrorism Policing, 'Together, we're tackling online terrorism' (*Counter Terrorism Policing*, 19 December 2018) <https://www.counterterrorism.police.uk/together-were-tackling-online-terrorism/> accessed 16 February 2020.

which proposed making internet companies responsible for harmful and illegal content as well as an introduction of a new regulator with enforcement authority.[2379] The government is still working on the proposed changes, having published the latest consultation on the issue on 12 February 2020.[2380]

As the UK has recently entered the Brexit transition period, it was questioned whether the UK will keep the current rules under the General Data Protection Regulation 2018 ('GDPR'). After the 31 December 2020, the UK government will introduce the UK GDPR, which will merge the GDPR with the Data Protection Act 2018. There is very little difference between the original and proposed document, which is likely to uphold the current standards of freedom of expression online in the UK.

The Right to be Forgotten will still have precedence in the UK – at least for the time being. The Great Repeat Bill will provide the UK courts with the ability to refer to EU courts' rulings when interpreting UK's EU-derived laws.

The UK will continue to be a member of the Council of Europe, which, of course, is separate from the EU. Consequently, it will still be bound by Article 10 of the European Convention on Human Rights.[2381]

10.2 Disadvantages of the current system

There is a lack of law in the UK, which requires blocking of internet content by ISPs in the fields of privacy law. There is a number of injunctions that might be applied in this situation, which they can only place indirect requirements to block access to the internet.[2382] Yet in light of high-profile cases, such as *Venables v News Group Newspapers Ltd,*[2383] the UK law perhaps needs a more concrete regulation.

There is no particular UK organisation that monitors the overall compliance with the law on the internet. The ORG created a list of 23 private and public entities aimed at a specific part of the internet regulation.[2384] They all operate in a different way, often without sufficient policies and rarely collaborating with

[2379] Secretary of State for Digital, Culture, Media & Sport, *Online Harms White Paper* (CP 57, 2019).
[2380] ibid.
[2381] Open Rights Group, 'Freedom of Expression – Open Rights Group Brief' (2019) 2.
[2382] Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' [2015] 760.
[2383] *Venables v News Group Newspapers Ltd* [2001] 1 All England Law Reports 908.
[2384] Open Rights Group, 'UK Internet Regulation – Part 1: Internet Censorship in the UK today' (2018) 17.

each other. Consequently, overseeing the internet content is usually done under voluntary and informal procedures[2385]

Only unlawful terrorist materials and defamatory statements can be subject to statutory 'notice and take-down' procedures (see section 2.2). Yet, even these provisions do not require intermediaries to assess whether the content complies with the law. CTIRU does not monitor the internet but encourages the public to report on such illegal materials. In today's world of the high terrorism threats, one needs to answer a question whether it is appropriate to leave such an important role to the public. On the contrary, IWF, on top of their hotline, hire highly-trained analysists, who assess more than 1,000 webpages weekly.[2386] Their achievements prove that such a solution is not only possible but also effective.

IWF, however, does not disclose the materials that had been removed on the basis of being unlawful. The URL blacklist is being kept secret and IWF is not under any obligation to inform the page owner in case their page was included on the list. [2387] Nowadays, online domains often contain some sort of intellectual property on it and sudden removal of it can be disproportionate and unfair. As the organisation deals with some extremely sensitive cases, it is very challenging to strike a correct balance. Yet, more attention should be given whether the owners of the online domain get enough protection under the current regulations.

11. How do you overall assess the legal situation in your country regarding internet censorship?

The extent of internet censorship is concerning to some degree. The balance is truck between the fact that the government had imposed relatively few filters on internet channels, however, the political climate has encouraged ISPs to engage in filtering and blocking to a large extent. The lack of legal provisions has a negative side effect, where the reality is that many individuals and companies affected by the ISP blocking tactics have few direct routes to seek redress from the courts, and are forced to rely on ad hoc solutions.

It is interesting to note that in 2014, Reporters Without Borders described the United Kingdom as an enemy of the internet, and the degree of filtering and

2385 Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' [2015] 772.

2386 Internet Watch Foundation, 'What we do' <https://www.iwf.org.uk/what-we-do> accessed 15 February 2020.

2387 Wolfgang Benedek and Matthias C. Kettemann, *Freedom of Expression and the Internet* (Council of Europe, 2014).

blocking by ISPs has only increased in the interim. Reporters Without Borders argued that,

Three of the entities that Reporters Without Borders has named as Enemies of the Internet are located in democracies that have traditionally claimed to defend Freedom of Expression and the free flow of information. The NSA in the United States, GCHQ in the United Kingdom and the Centre for Development of Telematics in India are no better than their Chinese, Russian, Iranian or Bahraini counterparts.[2388]

In response to this, the Communications Select Committee set up an inquiry in 2017 to determine how internet regulation in the UK should operate. In its report, titled 'Regulating in a digital world' the committee noted that, over a dozen UK regulators have a remit covering the digital world but there is no body which has complete oversight. As a result, regulation of the digital environment is fragmented, with gaps and overlaps. Big tech companies have failed to adequately tackle online harms.[2389]

In light of this report, it is abundantly clear that the legal situation regarding internet censorship in the UK is lacking and in need of reform.

[2388] Reporters Without Borders, 'Enemies of the Internet 2014: entities at the heart of censorship and surveillance', (March 11th 2014), <https://rsf.org/en/news/enemies-internet-2014-entities-heart-censorship-and-surveillance> accessed 28 February 2020.

[2389] Parliament.uk, 'It is time to rein in big tech, says Lords committee', 09 March 2019, <https://www.parliament.uk/business/committees/committees-a-z/lords-select/communications-committee/news-parliament-2017/internet-regulation-report-publication/> accessed 20 February 2020.

Conclusion

In conclusion the current state of the United Kingdom's legislation relating to the internet censorship and the freedom of expression varies. The current legislation tries to protect everyone; however, it is maybe overprotective. A fast reform is definitely needed, since the legislation lacking certain element.

Table of legislation

Title of the legal act	Provision text in English Language
Communications Act 2003 s.21	1. "It shall be the duty of OFCOM, in accordance with the following provisions of this section, to exercise their powers under paragraph 14 of the Schedule to the Office of Communications Act 2002 (c. 11) (committees of OFCOM) to establish and maintain a committee to provide the advice specified in this section."
Copyright, Designs and Patents Act 1998 s.97 s.97A	1. **"s97** (1)Where in an action for infringement of copyright it is shown that at the time of the infringement the defendant did not know, and had no reason to believe, that copyright subsisted in the work to which the action relates, the plaintiff is not entitled to damages against him, but without prejudice to any other remedy. (2)The court may in an action for infringement of copyright having regard to all the circumstances, and in particular to— (a)the flagrancy of the infringement, and (b)any benefit accruing to the defendant by reason of the infringement, award such additional damages as the justice of the case may require." 2. "s.97A"(1)The High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright. (2)In determining whether a service provider has actual knowledge for the purpose of this section, a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, amongst other things, shall have regard to— (a)whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c) of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013); and (b)the extent to which any notice includes— (i)the full name and address of the sender of the notice; (ii)details of the infringement in question. (3)In this section " service provider " has the meaning given to it by regulation 2 of the Electronic Commerce (EC Directive) Regulations 2002.] 2."
Defamation Act 2013 s.1 s.10 s.5ss.12 s.13	1. "1Serious harm (1)A statement is not defamatory unless its publication has caused or is likely to cause serious harm to the reputation of the claimant. (2)For the purposes of this section, harm to the reputation of a body that trades for profit is not "serious harm" unless it has caused or is likely to cause the body serious financial loss."

	2. "10Action against a person who was not the author, editor etc (1)A court does not have jurisdiction to hear and determine an action for defamation brought against a person who was not the author, editor or publisher of the statement complained of unless the court is satisfied that it is not reasonably practicable for an action to be brought against the author, editor or publisher. (2)In this section "author", "editor" and "publisher" have the same meaning as in section 1 of the Defamation Act 1996." 3. "The defence under this section is not defeated by reason only of the fact that the operator of the website moderates the statements posted on it by others." 4. "13Order to remove statement or cease distribution etc (1)Where a court gives judgment for the claimant in an action for defamation the court may order— (a)the operator of a website on which the defamatory statement is posted to remove the statement, or (b)any person who was not the author, editor or publisher of the defamatory statement to stop distributing, selling or exhibiting material containing the statement. (2)In this section "author", "editor" and "publisher" have the same meaning as in section 1 of the Defamation Act 1996. (3)Subsection (1) does not affect the power of the court apart from that subsection."
Digital Economy Act 2017 s.30	1. "30Interpretation and general provisions relating to this Part (1)In this Part— "the age-verification regulator" means the person or persons designated as the age-verification regulator under section 16; "extreme pornographic material" has the meaning given in section 22; "internet service provider" means a provider of an internet access service within the meaning given in Article 2 of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015; "pornographic material" has the meaning given in section 15; "turnover" has the meaning given in section 20(15). (2)Section 22(3) of the Video Recordings Act 1984 (effect of alterations) applies for the purposes of this Part as it applies for the purposes of that Act. (3)Nothing in this Part affects any prohibition or restriction in relation to pornographic material or extreme pornographic material, or powers in relation to such material, under another enactment or a rule of law."
Electronic Commerce Directive 2000 Article 12.	"1. (12) It is necessary to exclude certain activities from the scope of this Directive, on the grounds that the freedom to provide services in these fields cannot, at this stage, be guaranteed under the Treaty or existing secondary legislation; excluding these activities does not preclude any instruments which might prove necessary for the proper functioning of the internal market; taxation, particularly value added tax imposed

	on a large number of the services covered by this Directive, must be excluded form the scope of this Directive."
European Convention on Human Rights 1950 Art 10	"1. ARTICLE 10 Freedom of expression 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."
Human Rights Act 1998 Sched 1 art 9, 10,14	"1. Article 9 Freedom of thought, conscience and religion 1Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance." 2 Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others." *2. "Article 10 Freedom of expression* 1Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary." 3. "*Prohibition of discrimination*

	The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."
Information Society Directive Art 8	1. "Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."
Official Secrets Act 1989 s.6	1. "Information entrusted in confidence to other States or international organisations. (1)This section applies where— (a)any information, document or other article which— (i)relates to security or intelligence, defence or international relations; and (ii)has been communicated in confidence by or on behalf of the United Kingdom to another State or to an international organisation, has come into a person's possession as a result of having been disclosed (whether to him or another) without the authority of that State or organisation or, in the case of an organisation, of a member of it; and (b)the disclosure without lawful authority of the information, document or article by the person into whose possession it has come is not an offence under any of the foregoing provisions of this Act. (2)Subject to subsection (3) below, the person into whose possession the information, document or article has come is guilty of an offence if he makes a damaging disclosure of it knowing, or having reasonable cause to believe, that it is such as is mentioned in subsection (1) above, that it has come into his possession as there mentioned and that its disclosure would be damaging. (3)A person does not commit an offence under subsection (2) above if the information, document or article is disclosed by him with lawful authority or has previously been made available to the public with the authority of the State or organisation concerned or, in the case of an organisation, of a member of it. (4)For the purposes of this section "security or intelligence", "defence" and "international relations" have the same meaning as in sections 1, 2 and 3 above and the question whether a disclosure is damaging shall be determined as it would be in relation to a disclosure of the information, document or article in question by a Crown servant in contravention of section 1(3), 2(1) and 3(1) above. (5)For the purposes of this section information or a document or article is communicated in confidence if it is communicated on terms requiring it to be held in confidence or in circumstances in which the person communicating it could reasonably expect that it would be so held."

Protection of Children Act 1978 s.1ss.1	1. [F1Subject to sections 1A and 1B,] it is an offence for a person— (a)to take, or permit to be taken [F2or to make], any indecent photograph [F2or pseudo-photograph] of a child F3. . .; or (b)to distribute or show such indecent photographs [F4or pseudo-photographs]; or (c)to have in his possession such indecent photographs [F4or pseudo-photographs], with a view to their being distributed or shown by himself or others; or (d)to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs [F4or pseudo-photographs], or intends to do so."
Racial and Religious Hatred Act 2006 c.1.s.1	1. "Hatred against persons on religious grounds The Public Order Act 1986 (c. 64) is amended in accordance with the Schedule to this Act, which creates offences involving stirring up hatred against persons on religious grounds."
Sexual Offences Act 2003 s.46	1. "46Criminal proceedings, investigations etc. (1)After section 1A of the Protection of Children Act 1978 (c. 37) insert— **"**1BException for criminal proceedings, investigations etc. (1)In proceedings for an offence under section 1(1)(a) of making an indecent photograph or pseudo-photograph of a child, the defendant is not guilty of the offence if he proves that— (a)it was necessary for him to make the photograph or pseudo-photograph for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings, in any part of the world, (b)at the time of the offence charged he was a member of the Security Service, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of the Service, or (c)at the time of the offence charged he was a member of GCHQ, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of GCHQ. (2)In this section "GCHQ" has the same meaning as in the Intelligence Services Act 1994." (2)After Article 3 of the Protection of Children (Northern Ireland) Order 1978 (S.I. 1978/1047 (N.I. 17)) insert— **"**3AException for criminal proceedings, investigations etc. (1)In proceedings for an offence under Article 3(1)(a) of making an indecent photograph or pseudo-photograph of a child, the defendant is not guilty of the offence if he proves that— (a)it was necessary for him to make the photograph or pseudo-photograph for the purposes of the prevention, detection or investigation of crime, or for the purposes of criminal proceedings, in any part of the world,

	(b)at the time of the offence charged he was a member of the Security Service, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of the Service, or (c)at the time of the offence charged he was a member of GCHQ, and it was necessary for him to make the photograph or pseudo-photograph for the exercise of any of the functions of GCHQ. (2)In this Article "GCHQ" has the same meaning as in the Intelligence Services Act 1994."
Terrorism Act 2006 s.3	1. "For the purposes of this section, the statements that are likely to be understood by members of the public as indirectly encouraging the commission or preparation 11. "s 3Application of ss. 1 and 2 to internet activity etc. (1)This section applies for the purposes of sections 1 and 2 in relation to cases where— (a)a statement is published or caused to be published in the course of, or in connection with, the provision or use of a service provided electronically; or (b)conduct falling within section 2(2) was in the course of, or in connection with, the provision or use of such a service. (2)The cases in which the statement, or the article or record to which the conduct relates, is to be regarded as having the endorsement of a person ("the relevant person") at any time include a case in which— (a)a constable has given him a notice under subsection (3); (b)that time falls more than 2 working days after the day on which the notice was given; and (c)the relevant person has failed, without reasonable excuse, to comply with the notice. (3)A notice under this subsection is a notice which— (a)declares that, in the opinion of the constable giving it, the statement or the article or record is unlawfully terrorism-related; (b)requires the relevant person to secure that the statement or the article or record, so far as it is so related, is not available to the public or is modified so as no longer to be so related; (c)warns the relevant person that a failure to comply with the notice within 2 working days will result in the statement, or the article or record, being regarded as having his endorsement; and (d)explains how, under subsection (4), he may become liable by virtue of the notice if the statement, or the article or record, becomes available to the public after he has complied with the notice. (4)Where— (a)a notice under subsection (3) has been given to the relevant person in respect of a statement, or an article or record, and he has complied with it, but (b)he subsequently publishes or causes to be published a statement which is, or is for all practical purposes, the same or to the same effect as the statement to which the notice related,

	or to matter contained in the article or record to which it related, (a "repeat statement"); the requirements of subsection (2)(a) to (c) shall be regarded as satisfied in the case of the repeat statement in relation to the times of its subsequent publication by the relevant person. (5)In proceedings against a person for an offence under section 1 or 2 the requirements of subsection (2)(a) to (c) are not, in his case, to be regarded as satisfied in relation to any time by virtue of subsection (4) if he shows that he— (a)has, before that time, taken every step he reasonably could to prevent a repeat statement from becoming available to the public and to ascertain whether it does; and (b)was, at that time, a person to whom subsection (6) applied. (6)This subsection applies to a person at any time when he— (a)is not aware of the publication of the repeat statement; or (b)having become aware of its publication, has taken every step that he reasonably could to secure that it either ceased to be available to the public or was modified as mentioned in subsection (3)(b). (7)For the purposes of this section a statement or an article or record is unlawfully terrorism-related if it constitutes, or if matter contained in the article or record constitutes— (a)something that is likely to be understood, by any one or more of the persons to whom it has or may become available, as a direct or indirect encouragement or other inducement to the commission, preparation or instigation of acts of terrorism or Convention offences; or (b)information which— (i)is likely to be useful to any one or more of those persons in the commission or preparation of such acts; and (ii)is in a form or context in which it is likely to be understood by any one or more of those persons as being wholly or mainly for the purpose of being so useful. (8)The reference in subsection (7) to something that is likely to be understood as an indirect encouragement to the commission or preparation of acts of terrorism or Convention offences includes anything which is likely to be understood as— (a)the glorification of the commission or preparation (whether in the past, in the future or generally) of such acts or such offences; and (b)a suggestion that what is being glorified is being glorified as conduct that should be emulated in existing circumstances. (9)In this section "working day" means any day other than— (a)a Saturday or a Sunday; (b)Christmas Day or Good Friday; or (c)a day which is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80) in any part of the United Kingdom.

The Electronic Commerce (EC Directive) Regulations 2002 Regulation 19	1. Hosting **"19.** Where an information society service is provided which consists of the storage of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage where— (a)the service provider— (i)does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or (ii)upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, and (b)the recipient of the service was not acting under the authority or the control of the service provider."
Universal Declaration of Human Rights 1948, United Nations. Article 19.	1. Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Bibliography

English titles

Legislation

Communications Act 2003

Copyright, Designs and Patents Act 1998

Coroners & Justice Act 2009

Criminal Justice & Immigration Act 2008

Criminal Justice & Public Order Act 1994

Defamation Act 1996

Defamation Act 2013

Digital Economy Act 2010

Digital Economy Act 2017

Electronic Commerce Directive 98/34/Ec

European Convention on Human Rights 1950

Human Rights Act 1998

Information Society Directive

Official Secrets Act 1989

Protection of Children Act 1978

Racial and Religious Hatred Act 2006

Sexual Offences Act 2003

Terrorism Act 2006

The Electronic Commerce (EC Directive) Regulations 2002

Universal Declaration of Human Rights 1948, United Nations.

Reports

Council of Europe, 'Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content' [2015] 13

Council of Europe, Comparative Study On Blocking, Filtering And Take-Down Of Illegal Internet Content, Lausanne, 20 December 2015.

Google Transparency Report. Turkey.

Http://Www.Google.Com/Transparencyreport/Removals/ Government/Tr/ For Example In The January-June 2013 Reporting Period: "We Received 1,126 Requests

From Government Agencies To Remove A Total Of 1,345 Items From Blogger, Google+, And Web Search That The Agencies Claimed Were In Violation Of Law 5651. We Removed 188 Items That Violated Our Product Policies." Also See: Jeff Landale. Google Transparency Report Sheds Light on Internet Threats. 6 December 2012. R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role of Internet Intermediaries. Other Publications from The Centre for Global Communication Studies

Home Office, 'Hate crime action plan: Challenge it, Report it, Stop it' [2012] 10

Internet Watch Foundation, '2018 Annual Report' [2018]

Ministry of Justice, Complaints about defamatory material posted on websites: Guidance on Section 5 of the Defamation Act 2013 and Regulations, (January 2014).

Open Rights Group, 'Freedom of Expression – Open Rights Group Brief' (2019)

Open Rights Group, 'UK Internet Regulation – Part 1: Internet Censorship in the UK today' (2018)

Open Rights Group, 'UK Internet Regulation Part I: Internet Censorship In The UK Today'

Secretary of State for Digital, Culture, Media & Sport, Online Harms White Paper (CP 57, 2019)

Books

R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role of Internet Intermediaries. Other Publications from The Centre for Global Communication Studies Global Network Initiative Implementation Guidelines.

R. Mackinnon; E. Hickok, Lonnai; B, Allon; And L. Hai-In. (2015). Fostering Freedom Online: The Role Of Internet Intermediaries. Other Publications from The Centre For Global Communication Studies

Journals

T.J. McIntyre, 'Blocking child pornography on the Internet: European Union developments', International Review of Law Computers & Technology, November 2010.

A. Mary, 'Internet Copyright Infringement Liability: Is an Online Access Provider More Like A Landlord or A Dance Hall Operator' (1997) 27 Golden Gate University Law Review.

Benedek, Wolfgang and Matthias C. Kettemann, Freedom of Expression and the Internet, Council of Europe Publishing, December 2013, 190.

Emily Laidlaw, 'The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation' [2012] International Journal of Law and Information Technology 20(4)

Ginsberg, Jodie. 'Balancing Privacy and Free Expression Online' (June 2016) Infotoday.

Gov.UK, 'How to make a freedom of information (FOI) request'(2020) Freedom of Information Act 2000, https://www.gov.uk/make-a-freedom-of-information-request

Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003

Paul Sandle, 'UK to make social media platforms responsible for harmful content – BBC' Thomas Reuters, Technology News, February 12 (2020).

Wolman, Andrew. 'Combating Hate Speech at the Local Level: A Comparison of East Asian and European Approaches' (November 18 2019) Nordic Journal of Human Rights, 87-104

Periodicals

Murray, Daragh. 'Freedom of Expression, Counter-Terrorism and the Internet in Light of the UK Terrorist Act 2006 and the Jurisprudence of the European Court of Human Rights' (2009) 27 Neth Q Hum Rts 331

Digital resources

Baroness Williams of Trafford, 'Islam: Tenets – Question' (TheyWorkForYou, 7 December 2017)
<https://www.theyworkforyou.com/lords/?id=2017-12-07c.1280.3>
accessed 15 February

Bart Cammaerts & Bingchun Meng, 'The government's new Digital Economy Act will do little to prevent file sharing – the music industry must continue to innovate online if it is to survive' LSE GovBlog, <https://blogs.lse.ac.uk/politicsandpolicy/digital-economy-act-file-sharing-music-industry/> accessed 10 February 2020.

Ben Rooney. Microsoft Google Join To Battle Child Porn. Wall Street Journal. 18 November 2013.
<Http://Online.Wsj.Com/News/Articles/Sb10001424052702304439804579205874211710440> (Accessed 10th of February 2020.)

Brian Chang, 'From Internet Referral Units to International Agreements: Censorship of the Internet by the UK and EU, Columbia Human Rights Law Review, (January 2018)

Counter Terrorism Policing, 'Together, we're tackling online terrorism' (Counter Terrorism Policing, 19 December 2018)
<https://www.counterterrorism.police.uk/together-were-tackling-online-terrorism/>
accessed 16 February 2020

Facebook Terms Of Service Https://Www.Facebook.Com/Terms Accessed Yahoo Terms Of Service <Https://Policies.Yahoo.Com/Us/En/Yahoo/Terms Accessed >

Faq<Http://Www.Google.Com/Transparencyreport/Removals/Copyright/Faq/> Accessed 31 March 2013, For The Period Between July And December 2011, Google States That It 'Removed 97% Of Search Results Specified In Requests'.

Google Transparency Report

Google Terms Of Services
Https://Www.Google.Com/Policies/Terms/> Accessed

Home Affairs Select Committee, 'Hate and abuse on social media'
<https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/60904.htm> accessed 15 February 2020

<Http://Expandedramblings.Com/Index.Php/By-The-Numbers-A-Gigantic-List-Of-Google-Stats-Andfacts. >

<https://doi-org.ezproxye.bham.ac.uk/10.1017/CBO9780511763410 >

<Https://Globalnetworkinitiative.Org/Implementationguidelines/Index.Php>
107 Demands to Remove or Filter Content.

Index on Censorship, 'Adopt a 'human rights by design' approach towards regulating online content, say civil society groups' (Index, 16 October 2016)
<https://www.indexoncensorship.org/2018/10/adopt-a-human-rights-by-design-approach-towards-regulating-online-content-say-civil-society-groups/>
accessed 16 February 2020

Internet Watch Foundation, 'FC Code of Practice' <https://www.iwf.org.uk/what-we-do/who-we-are/governance/funding-council/fc-code-of-practice>
accessed 15 February 2020

Internet Watch Foundation, 'Our remit and vision' <https://www.iwf.org.uk/what-we-do/why-we-exist/our-remit-and-vision> accessed 15 February 2020

Internet Watch Foundation, 'URL List' <https://www.iwf.org.uk/become-a-member/services-for-members/url-list> accessed 15 February 2020

Internet Watch Foundation, 'What we do' <https://www.iwf.org.uk/what-we-do> accessed 15 February 2020

Internet Watch Foundation, 'What we do', (2020) <https://www.iwf.org.uk/what-we-do>

Jasper Jackson, 'ISPs that restrict porn or block ads could be breaking EU guidelines', (The Guardian, 31st August 2016).
<https://www.theguardian.com/media/2016/aug/31/isps-porn-block-ads-eu-guidelines-sky-bt-talktalk-o2> Accessed 14 February 2020. Reporters Without Borders, 'Enemies of the Internet 2014: entities at the heart of censorship and surveillance', (March 11th 2014), <https://rsf.org/en/news/enemies-internet-2014-entities-heart-censorship-and-surveillance> accessed 28 February 2020.

M. Chris Lecture Document Dated 12.10.2017 (Week 5 Of 2017-2018)

Marsden, Christopher T. Internet Co-Regulation, Cambridge University Press, (2011), DOI:

Reporters Without Borders, '2019 World Press Freedom Index'
<https://rsf.org/en/ranking> accessed 16 February 2020

Sandle.P, Britain to make social media platforms responsible for harmful content,<<https://in.reuters.com/article/britain-tech-regulation/uk-to-make-social-media-platforms-responsible-for-harmful-content-bbc-idINKBN2060RC >>
(Accessed on the 12th of February 2000)

Sir John Hayes MP, 'Counter-Terrorism: Written Question – 30893', (Parliament.uk. 14 March 2016), <https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-03-14/30893/> accessed 04 January 2020.

Smith C. By The Numbers: 40 Amazing Google Stats And Facts. Digital Marketing Ramblings.

Smith C. By The Numbers: 40 Amazing Google Stats And Facts. Digital Marketing Ramblings.
<Http://Expandedramblings.Com/Index.Php/By-The-Numbers-A-Gigantic-List-Of-Google-Stats-Andfacts>

Case law

(1) NT1 & (2) NT2 v Google LLC [2018] EWHC 799

Byrne V Deane (1937 1 Kb 818)

Godfrey v Demon [1999] Entertainment and Media Law Reports 54

Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez (Case C-131/12)

Handyside v the United Kingdom [1976] 12 WLUK 53

R v Bowden [2000] 2 All ER 418

Richardson V Facebook (2015) [2015] Ewhc 3154 (Qb)

Tamiz v the United Kingdom App no 3877/14 (ECtHR, 19 September 2017)

Twentieth Century Fox and others v British Telecommunications plc [2011] EWHC 1981

Venables v News Group Newspapers Ltd [2001] 1 All England Law Reports 908

International Report on Internet Censorship

International Focus Programme on Law and Technology

Final Report of the International Legal Research Group on Internet Censorship (eds)

The international report on Internet Censorship provides the reader with a comprehensive overview of regulation of freedom of expression online across 24 different European jurisdictions. The report discusses the concept of censorship and its boundaries with the right to information. The report explores regulation of blocking and takedown of internet content, particularly whether specific legislation on the issue exists and if the area is self-regulated in each country. Furthermore, the report includes analyses of the right to be forgotten in each of the participating countries and finally the regulation of the liability of internet intermediaries. Each analysis looks into both existing regulations and policy papers as well as any cases that may exist on the topic.

In addition to the analyses, the report assesses how the legislation regarding blocking and takedown of online content, liability of internet intermediaries and the right to be forgotten will develop in each country over the coming five-year period. Finally, the report assesses balancing issues in terms of reaching a balance between allowing freedom of expression online and protecting against online hate speech as well as protecting other rights online.

The report is an excellent tool for students, academics and practitioners who wish to gain an overview of European policies, regulation and case law regarding freedom of expression online. Furthermore, the report serves as a great starting point for further research as it contains tables with translation of relevant legislation, literature and jurisprudence.

elsa
The European Law Students' Association

ELSA LEGAL RESEARCH GROUPS

9 789462 406469 >