No. 69· I - 2021

SYNERGY MAGAZINE

Magazine of the European Law Students' Association

PRIVACY AND HUMAN RIGHTS IN THE DIGITAL ERA

elsa
The European Law Students' Association

ABOUT ELSA

ELSA International
Phone: +32 2 646 26 26
Web: www.elsa.org
E-mail: elsa@elsa.org

The European Law Students' Association

The Association

The European Law Students' Association, ELSA, is an international, independent, non-political and not-for-profit organisation comprised of and run by and for law students and young lawyers. Founded in 1981 by law students from Austria, Hungary, Poland and West Germany, ELSA is today the world's largest independent law students' association.

Synergy Magazine

Synergy Magazine is ELSA's members' magazine, which is published digitally twice a year and read across law students and young lawyers. The articles are contributions from students, young and experienced lawyers as well as academics.

VISION "A JUST WORLD IN WHICH THERE IS RESPECT FOR HUMAN DIGNITY AND CULTURAL DIVERSITY"

ELSA's Members

ELSA's members are internationally minded individuals who have an interest in foreign legal systems and practices. Through our activities, such as seminars, conferences, law schools, moot court competitions, legal writing, legal research and the Student Trainee Exchange Programme, our members acquire a broader cultural understanding and legal expertise.

Our Special Status

ELSA has gained a special status with several international institutions. In 2000, ELSA was granted Participatory Status with the Council of Europe. ELSA has Consultative Status with several United Nations bodies: UN ECOSOC, UNCITRAL, UNESCO & WIPO.

ELSA is present in 44 countries

Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Montenegro, the Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, Russia, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine and the United Kingdom.

ELSA Members x 60,000

ELSA Local Groups x 400

ELSA National Groups x 44

ELSA International

Human Rights Partner

General Legal Partners

General Education Partners

General Partners

SYNERGY Magazine
Editor-in-chief: Nikos Fifis
Assistant Editor: Aretina Stefani
Linguistic Editor: Maisie Beavan
Design : Nikos Fifis
Contact: marketing@elsa.org

Contributions

Would you like to contribute with articles or pictures for the Magazine? Please, contact ELSA International for further information and guidelines.

Advertising

Would you like to advertise your courses, services, company or products, please do not hesitate to contact ELSA .

ISSN 0250-7129

EDITORIAL

Nikos Fifis
Vice President in charge of Marketing of the International Board 2020/21

Digital communications technologies have become part of our everyday life. By dramatically improving access to information and real-time communication, innovations in communications technology have enhanced freedom of expression, facilitated global debate and promoted democratic participation. By amplifying the voices of human rights defenders and providing them with new tools to document and expose abuses, these powerful technologies offer the promise of improved enjoyment of human rights. In the digital era, however, communications technologies also have enhanced the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection with deep concerns arising regarding policies and practises exploiting the vulnerability coming hand in hand with the digital world to violate a fundamental human right, the right to privacy. This edition of Synergy will shed light on many aspects of this interesting legal enigma and specific topics like data masking, video surveillance of prisoners and the right to be forgotten.

Vehemently protecting human rights in any form, standing for human dignity and cultural diversity and yielding passionate young lawyers the platform and opportunities to develop personally and professionally and make the world a better place, are the values and visions which keep the ELSA flame burning for 40 consecutive years now, even in darker times like the one the whole world is currently experiencing. This realisation has served as my fuel and inspiration during this very special year with everything being remote and digital when the countless hours being spent in front of the computer screen have started taking their toll. However, looking back to the remote traineeships, virtual moot court competitions, virtual international internal meetings and many more, I can only express my awe and pride for the enthusiasm, adaptability and all the amazing things our network has achieved throughout this challenging year, making my IB experience very rewarding and special.

I would like to end this farewell with a few well-deserved words of thanks and gratitude. Firstly, I would like to extend a big thank you to my Assistant Editor for Synergy, Aretina Stefani, for doing an outstanding job in helping editing and improving this magazine. Secondly, I want to express my gratitude and appreciation for the whole ELSA International Team for their talent, passion and sustained effort to keep the efficiency and team spirit up over this puzzling, online year. It has been a pleasure working with such a dynamic team and I am so lucky to have had this opportunity.

But most importantly, I wish to wholeheartedly thank the International Board of ELSA 2020/2021, my Boardies, who are neither my colleagues, nor friends, but my family. Thank you for your endless love and support, for seeing light over this pandemic darkness, for helping me grow both professionally and personally. Although we will soon embark on different journeys, I am sure we will all be forever cherishing this experience as one of the most challenging, unexpected, gratifying and happy years of our careers.

It is never easy saying goodbye, but it is more pleasant when I know my absence will not leave a huge void. So even though my term in ELSA is coming to an end, Tony will be taking the helm, making for a seamless transition. Best of luck Tony!

According to the Cambridge English Dictionary, Synergy makes for the combined power of a group when they are working together that is greater than the total power achieved by each working separately & the 69th edition of the Synergy Magazine accords perfectly to this definition. Dig in to explore the implications of privacy violations to human rights in the digital era as well as what has the ELSA Network been up to over this term of digitalized, working-from-home reality.

Have a good read!

TABLE OF CONTENTS

HIGHLIGHTS

Privacy & Human Rights in a Digital Era 14

Right to Be Forgotten 37

Children's Right to Privacy & Data Protection in a Digital Era 46

PARTNERS' AND EXTERNALS' PERSPECTIVE

INTERNATIONAL FOCUS

THINK GLOBAL, ACT LOCAL

Privacy

PRIVACY IN THE DIGITAL ERA: FACE/ING THE FUTURE

Sophie Kwasny
Head of the Data Protection Unit
Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Robust and well-established elements of responses to new challenges

The right to privacy – referred to in European law as the right to respect for private life – emerged in international human rights law in the Universal Declaration of Human Rights (UDHR), adopted in 1948. Soon after the adoption of the UDHR, Europe affirmed this right in the European Convention on Human Rights, which dates back to 1950.

Is this multi decades old human right still relevant today, in an age of digital transformation, artificial intelligence, hyper-connectivity, blockchain, etc.?

The European Convention on Human Rights provides that everyone has the right to respect for his or her private and family life, home and correspondence. Interference with this right by a public authority is prohibited, except where the interference is in accordance with the law, pursues important and legitimate public interests and is necessary in a democratic society.

Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily 'negative' undertaking, there may be positive obligations inherent to an effective respect for private life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations between private parties.

The right to privacy, as others of the Convention, has been significantly developed by means of the interpretation of its provisions by the European Court of Human Rights. Through its case-law, the Court has made the Convention a living instrument and has extended the rights afforded, applying them to situations that were not foreseeable when the Convention was first adopted in 1950. This is what makes the right to privacy more relevant today than it might ever have been.

The processing of biometric data is a good example to take as it perfectly illustrates a technology that could hardly have been foreseen at such algorithmic scale over 70 years ago. Yes, the example deals with one specific type of processing of biometric data, which regularly hits the media headlines: facial recognition.

For Cicero, the face was the mirror of the soul. The close link between an image (today in the form of a computer template) and the deepest and unique intimacy of a person was already acknowledged thousands of years ago, when the potentialities – and risks – of biometrics could never be imagined. And

today? Facial recognition has become as present and widespread as governors were in the Roman Empire and the race for digital transformation pushes its further development and spread at rapid pace.

Limiting the datafication of our faces

Has the impact on our societies and on our democracies of facial recognition, which some present as a "neutral" technology, been considered the way it should have? Is this technology, which relies on highly sensitive information (biometric data uniquely identifying or authenticating a person) and powerful algorithms that learn to recognise the features and characteristics of faces as innocuous as some present it? What lies behind the use of those biometric templates, and what are the longer-term consequences of this datafication of our faces?

Facial recognition is the perfect illustration of some of the important challenges ahead of us, which concern our right to privacy, our right to data protection, as well as other human rights and fundamental freedoms. Let's for instance take the use of facial recognition to identify demonstrators in a public crowd: the importance of our freedom of assembly, of our freedom of expression, of our freedom of thought will also immediately come to our minds.

The troubling illustrations of this technology, which are already too many to mention, should prompt us in delineating a clear and robust framework on facial recognition, which could span from a prohibition or moratorium regarding certain uses, to strictly legally prescribed scenarios with safeguards commensurate to the existing risks of infringement of our human rights and fundamental freedoms. Our ultimate question being, what society do we want to live in? Societies relying on extended surveillance capacities? Societies in which human autonomy could no longer be spontaneous, and where human integrity would be distorted by digital monitoring?

We all have a role to play in responding to those questions: organising and stimulating democratic debate, participating in this essential reflection, adopting the corresponding legal framework, developing innovative technical tools that embed privacy and data protection by design, ensuring that our practices are in full compliance with the applicable requirements, ensuring that they are effectively applied, etc.

The Council of Europe, as a leading human rights organisation, also has its role to play. We have been at the forefront of the promotion and defense of human

rights, democracy and the rule of law for over seventy years. Over those years, we have been providing groundbreaking legal and political instruments to tackle the emerging challenges of our times, be it in data protection, cybercrime or bioethics, to only name a few.

And facial recognition makes no exception. As cities, regions, countries and continents consider using this technology for the multiple functionalities it offers, as our interconnected lives continue to feed the web with zettabytes of pictures of our faces, as our bodies become the key to open our cars, our homes, our phones, let us seize the consciousness of the choice we have to make.

A concrete (legal) tool: our data protection Guidelines on facial recognition

The Committee of our Data Protection Convention (more commonly known as 'Convention 108') decided that the topic was too serious not to be addressed. On 28 January, that is on data protection day (this year, this date also marked the 40th Anniversary of Convention 108), it adopted an important document. For 40 years, Convention 108 has influenced and shaped the protection of privacy and of data protection in Europe and beyond, notably through the impressive work of its Committee. This Committee has once again decided to be a frontrunner, contributing to this essential reflection by recalling the risks at stake and providing guidance on how to respect the rights for privacy and data protection in the context of facial recognition.

The Committee has adopted guidelines on facial recognition which contain specific measures that legislators and decision-makers, facial recognition developers, manufacturers and service providers, and entities using these technologies should take with respect to this technology. The Committee takes

a firm stand regarding the strict limitation by law of certain uses of facial recognition technologies, and in some circumstances even, recommending a prohibition of their use, where they could lead to discrimination (even more so as harmful biases are now abundantly documented) or rely on affect recognition.

The Committee of Convention 108 has focused its work on data protection implications, but as previously highlighted, questions raised by the use of this technology go much deeper into the foundations of our democracies as other human rights and fundamental freedoms can be dramatically at stake.

And as it is artificial intelligence that has multiplied the capacities of facial recognition, another crucial step towards a stronger protection of our societies in the digital era is the work currently underway in the Council of Europe on artificial intelligence, which should enable the preparation of the first legally binding international instrument on artificial intelligence.

For our societies of the digital era to reinforce their harmonious development, we need greater consideration of our unique human features and needs, and we need to remain in full control of our individual attributes.

Lessons in Data Democracy:

PRIVACY AND HEALTH DATA DURING THE COVID-19 PANDEMIC

Renée Cortés
Content & Communication Manager
IE Law School

Data is the currency of the modern world. With powerful tech companies constantly gathering and selling our personal information, data has become humanity's most important commodity to date. What's more, as AI continues to grow in capabilities and scope, data becomes even more valuable. These self-learning machine-powered algorithms require a continuous input of fresh data to learn and improve, facilitating the growth of new areas of technology and development. In this context, the tension between privacy and growth has never been more pronounced.

Before the pandemic, these discussions were beginning to move forward and new policy recommendations were starting to take shape. In Europe, the GDPR marked a significant step in the protection of individual's human rights by establishing a framework for the proper utilization and storage of our personal data. Slowly but surely it seemed as though governments were beginning to show signs of standing up to Big Tech. For example, in 2020 the US government launched an antitrust investigation into Facebook drawing comparisons to its behemoth case against Microsoft.

Yet once COVID-19 hit, governments across the world realised the value of gathering our personal information to monitor—and stem—the progression of the virus. Tracking the movement of citizens, who they interact with, and the places they visit are vital pieces of information for understanding how the virus spreads through communities. Many countries, including Spain, utilized their arsenal of constitutional measures to call a state of alarm, enabling the government to act quickly and decisively. Across Europe, state leaders established national tracing apps and encouraged citizens to download and use these handheld monitoring devices. Yet it is still not clear how and to what end these apps gather our personal data.

Within this context, we must decide how to create

a data democracy: a system whereby data can be harvested and used for good, while protecting our privacy and human rights. We must consider how tracing apps utilize our data: are encryptions used? Is data anonymized? What cybersecurity is in place to prevent hackers from reverse-engineering any anonymization or encryption? And looking forward to the end of the pandemic, will governments delete these vast banks of personal data they hold, or will they see an opportunity to plug the gap in public funds by selling it?

Selling health data for a profit is nothing new. Indeed companies have been successfully buying and selling personal data without checks or balances for years. As large social media companies track our data to better target the advertising they expose us to, so do a variety of companies purchase health data to develop and market a range of products. Consider insurance, banking and retail products. Feeding these sectors with general and specific information regarding your health including your gender, age, medication, weight, seasonal allergies, blood pressure, cholesterol, whether you're trying to get pregnant, have a weak bladder, or acne can enable developers to push targeted adverts to your devices and drive sales. If you frequently travel to a supermarket near your home to buy low-fat yoghurt, that could place you on a list for weight-loss adverts.

Intermediaries known as data brokers gather (legally or otherwise) and sell this information on to companies who dig through the information on offer to find patterns of behavior they can apply to their products

and marketing initiatives. The European Commission estimates the data market in Europe to be worth as much as €106.8bn in 2020. As the pandemic pushed us increasingly online, the living database held on each of us has only grown.

What regulations are in place to protect citizen's privacy rights? Currently, the most robust legal framework in place globally to provide data protection is the GDPR. At the heart of the GDPR are seven key principles: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles form the legislation's overarching framework, with the goal of helping data processors and controllers limit the range of data they collect from users. The regulation also empowers individuals to get their personal data erased where storage or processing is no longer necessary for the original purpose, if consent is withdrawn, there is no legitimate interest, or it was unlawfully processed to begin with. These powers put control back in citizens' hands, empowering them to pay closer attention to how, when and why they share their personal data.

There is no clear answer to resolve the tension between data privacy, profit and our digital needs. One thing is obvious: there is no going back. Data is such an intrinsic part of our everyday lives that it would be impossible to retrospectively implement a framework to protect and control the way we share and process information. Looking forward, it is essential that we research new and innovative ways to promote data democracy, protect our personal rights, and gain autonomy when it comes to data sharing. Governments are best placed to make these decisions, but perhaps the true heroes in this ongoing debate will be multilateral organizations such as the EU, who have the capacity, mechanisms and indeed the ambition to rethink the way data is gathered, processed and stored.

PRIVACY AND HUMAN RIGHTS IN A DIGITAL ERA

Gonçalo Saraiva Matias
Dean of the
Catolica Global School of Law

CATOLICA FACULDADE DE DIREITO
ESCOLA DE LISBOA

CATOLICA Global School of Law

The transition to the digital economy and the digital era brings many challenges to the legal teaching, research and practice.

Privacy as a human right was designed to protect individuals from the abusive interference in their private lives by the State and other powerful entities. In a way, privacy as a human right entailed creating a protective "bubble" around the individuals, making sure that private space would not be invaded. In a way, keeping the distance from the State and other powerful entities would in most cases be enough to satisfy the general right to protection of citizens regarding privacy.

The rise of the media and, in particular, of the tabloid media raised new and more complex questions regarding the right to privacy. Can a reporter, or a "paparazzo", invade private property and private spaces to get the "perfect" photo? How is getting a picture of an artist, a politician or royalty in bathing suits any relevant to the general public? And what if the picture portrays a situation that is morally or even legally unacceptable? These questions were drawing the attention of specialists in privacy law for decades. But the transition to the digital economy and the omnipresence of digitalization completely changed the nature of the debate.

Now cameras are everywhere, from streets to private property, to cell phones. No one is safe from being caught on camera anytime, being a celebrity or a private citizen, a politician or a University student. Everyone´s privacy is at risk in a more traditional way. The whole idea of privacy, protection of image, prohibition of capturing and circulating photo, and the like came to a totally different understanding.

If any changes came with the COVID-19 pandemic, the acceleration of the transition to digital economy and digitalization is certainly one of them.

Where one year ago it was normal to meet someone over the phone, now everyone is expecting to see the other person over a video meeting. And because we all spent part of the year in lockdowns, it became normal and acceptable that our homes are depicted in

the most solemn or professional situations. It became adequate to comment on the impressive bookshelf behind one's image or the nice family pictures that one forgot to hide. Not to mention that it is likely a screen shot of such meetings may well end up in social media, without any perception of the potential consequences.

To address such a new world, public agencies dealing with data protection often adopt a protectionist standpoint, reacting to the new reality as if we were still living in the XX century. That does not contribute to a correct regulation of the new phenomena nor to the authority such agencies should maintain over society, especially private entities and individuals. In fact, unlike in the past, the latter poses much more serious and undetectable threats to privacy than the States that were the concern of the traditional debates on privacy.

We should not be acting as if privacy no longer matters and everyone can expose whatever they want because live in glass homes where all became public. But we should not also ignore the reality and pretend we still live in a society where the only real threats are coming from "paparazzos" hanging on tree tops and cameras should be prohibited in metro stations or public streets, forgetting that we all carry one in every cell

phone and prohibiting smart phones is not an option.

At Catolica Global School of Law we brainstormed for a long time on the threats and opportunities of the Digital Economy with partners, law firms and big tech companies and decided to launch a highly innovative LL.M. program on "Law in a Digital Economy". The idea is to revisit several areas of law, from contracts to financial law, from data protection to IP, or human rights, and assess how these areas have been impacted by technology.

We have now the first cohort of students highly motivated and engaged, discussing all these issues with the very knowledgeable Professors from around the world. The result is inspiring and exciting: innovative and forward thinking, breaking barriers in a sophisticated and structured way.

The experience we have shows a possible path: instead of ignoring the challenges or refuse evolution, the reality must be faced, the problems addressed and solutions be searched in an innovative non-conventional way. That is the mission, first and foremost, of Universities, in particular of law schools, that should be now training the lawyers of the future.

That is the aim, the purpose and the "raison d´être" of the Catolica Global School of Law.

Smart Global Governance

Smart Global Governance is a European Software editor that helps individuals and organisations to do better and more every day in terms of ethic, compliance and controls

FOR (MULTI) COMPLIANCE MANAGEMENT FROM A TO Z

- Data privacy.
- cyber security *(PCI DSS, NIST, ...).*
- ISO.
- Anti-Bribery, Gift laws.
- ESG
- Internal process *(choice of modules).*

75%

GAINS

FROM 25% TO 75% IN PRODUCTIVITY

FOR THE AUTOMATION OF MANUAL AND REPETITIVE TASKS

connected to the 1500 most common professional software packages on the market *(Microsoft, Oracle, Service- Now ...).*

+ 20 000

Users in 100 countries

FOR THE SYSTEMIC CONTROL

Digitized control plans automatically populated by :

- external data *(databases, vendor risk management).*
- internal data *(workstations, databases, cloud) .*

3 months offered

for ELSA members

www.smartglobalgovernance.com

WELL-BEING IN THE DIGITAL AGE- THE NEED FOR THE RIGHT TO DISCONNECT

Maja Rajić
Vice President in charge of Academic Activities
International Board of ELSA 2020/2021

Personal free time is taken for granted until it is too late. Digital technologies have undoubtedly changed our everyday life even before pandemic times. However, work-life balance has been significantly affected by these circumstances in recent months. The internet and the means to access it have become integral to the lives of everyone – children, youth, and even people who were born before computers and smartphones were a real thing. They have transformed education and learning, the way we communicate and maintain friendships and even the concept of self-awareness. Subsequently, work communication and activity moved from the office to the internet space. Our day-to-day activities that were reserved for the office hours entered our personal space and affected our well-being to that extent that the "24/7 work ethic" has led to concerns that this behaviour is now linked to multiple health issues, such as depression and anxiety.[1]

Seismic changes of switching to working from home due to the global pandemic brought various social changes, including almost completely abandoning the conventional work-life boundaries and even silently accepting that "switching off from work means that we are lazy". That being said, the European Parliament has called for an EU law that grants workers the right to digitally disconnect from work without facing negative consequences in order to protect employees' fundamental right to disconnect from work and not to be reachable outside working hours.[2]

Although digital tools have increased efficiency and flexibility for employers and employees, they created an "on-call culture", since the employees are easily reachable anytime and anywhere now when more than 37% of workers in the EU work from home, according to the Eurofund survey from April 2020.[3] We all know that modern problems require modern solutions, therefore the parliamentarians argue that disconnecting from work should be a fundamental right and as Maltese Socialist lawmaker Alex Agius Saliba stated, we have to catch up with the new reality caused by the Covid-19 pandemic and the effect it has had on the way we work now.

1 *http://techgenix.com/right-to-disconnect/ (last accessed on 23 February 2021)*

2 *https://www.europarl.europa.eu/news/en/headlines/society/20210121STO96103/parliament-wants-to-ensure-the-right-to-disconnect-from-work (last accessed on 23 February 2021)*

3 *Eurofound (2020), Living, working and COVID-19, COVID-19 series, Publications Office of the European Union, Luxembourg.*

It may come as a shock to many of you, as it came to me, that there is currently no specific European legal framework that directly defines and regulates this very needed right to disconnect. Principle 10 of the European Pillar of Social Rights calls for a healthy, safe and well-adapted work environment and for data protection, while Principle 9 calls for work-life balance. Besides the above mentioned principles, the Working Time Directive is indirectly related to the right to disconnect, as it defines inter alia maximum working hours and minimum daily and weekly rest periods.[4] Additionally, there are many initiatives at company level aiming to regulate the possible negative impacts of digital technologies on workers' lives.

To make sure that such an important change-and unfortunately overseen human right-does not get lost in discussions, the Committee on Employment and Social Affairs adopted a report calling on the European Commission to adopt a legislative proposal for a directive on the right to disconnect.[5] Besides defining the right to disconnect, the report sets minimum requirements on the use of digital tools for professional purposes as well as minimum requirements for remote work.

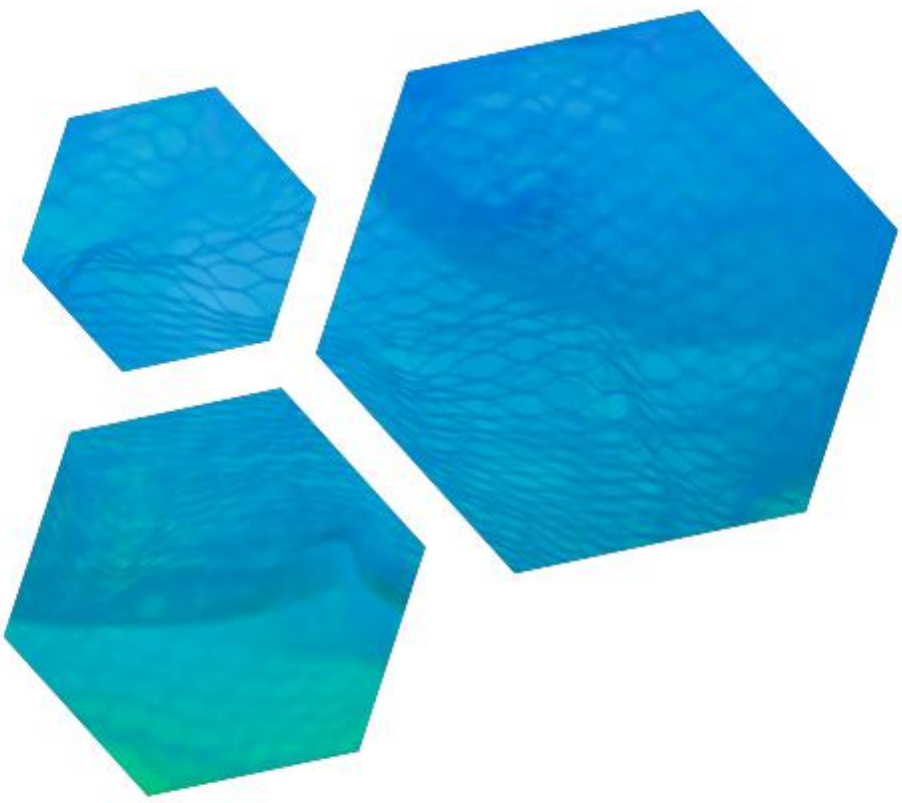
Why is the right to disconnect such an important human right, and more importantly, did a global pandemic have to happen in order for this right to be recognised? It was exceptional to contact an employee outside working hours or weekends or holidays twenty years ago. However, with the usage of digital technologies, employees are contacted by email or phone outside working hours and the unhealthy practice of being "on call" is slowly becoming the new norm nowadays.

The main question is – do we want to work in an environment where time off is a luxury and prioritising one's mental health is perceived as a "princess attitude"? On the other hand, do we want to be employers that do not respect the private life of their colleagues? I cannot provide you with answers to those questions, but I know that I want my free time and private life, or at least the "leftovers" of privacy, to stay mine as long as possible and, therefore, I welcome the initiative of European parliamentarians with hands wide open.

4 *Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time, 4 November 2003.*
5 *https://www.europarl.europa.eu/doceo/document/A-9-2020-0246_EN.html (last accessed on 23 February 2021)*

ALGORITHM - OPTIMISATION OR LACK OF AUTONOMY IN THE INFORMATION SOCIETY?

Carlos Eduardo Pereira
Treasurer
International Board of
ELSA 2020/2021



It's almost unanimous that social media changed the way we consume news, due to the fact that, according to Forbes, social media platforms became the main source of news with more than 2.4 billion internet users, in which nearly 64,5% of these receive breaking news from a social network, like Whatsapp, Facebook, Twitter, Youtube or Instagram, rather than the traditional sources. It seems like most internet users receive the first information about a topic in these online environments, which is quite related to the fact that new generations are less connected with these traditional sources of information, such as TV, Newspapers, or Radio. This can be seen as something positive, since Social Networks can constitute not only an important sociability resource, but also an excellent knowledge acquisition tool and consequently cause positive impacts, given that their power is utilised appropriately and efficiently.

According to a research of Reuters Institute, the impact of social networks, "an accelerated move to mobile devices and an increased rejection of online advertising", comes hand in hand with factors that "are weakening the business models that make it possible to produce quality news". This could be argued to mirror the economic impacts of the technological development of these platforms, due to the fact that people block advertising and paying for news online is a small percentage of the news consumers. This trend, combined with the drop in circulation of printed newspapers and advertising, is leading to unemployment in the press sector.

When mentioning social media and the role of these technological sources of information, the focus should be shifted on one small, but still key element, the algorithm... This is a crucial component in charge of managing gigantic amounts of information, and on the other side, creating a relationship between the content and the user, in order to generate an output. This finite sequence of well-defined, computer-implementable instructional is based on the interests of users, and for each user, there is, therefore, a unique algorithm. "All around us, algorithms provide a kind of convenient source of authority, an easy way to delegate responsibility; a shortcut that we take without thinking," writes mathematician Hannah Fry in her 2018 book Hello World: Being Human in the Age of Algorithms.

The algorithms are not the same for each social network. To illustrate the point, on Facebook the value of a share is worth more than a value of a comment,

a comment is worth more than a like, and so on... Sometimes the algorithm also acts as the source of the publication, prioritising videos that are published directly on the social network, instead of videos that are shared through other sites, the most common being on Youtube.

Every time the user creates interactions with a computer or a smartphone connected to social media, these algorithms are prioritising the relevance of the information, and not ordering them by the timeline of the content. This is done for several reasons- loyalty of the users, expansion of their number and increase of some brands' commercial interest to name a few. What is clear here is the fact that these big technology companies are using these artificial intelligence elements to create new ways to identify a person's basic psychological traits.

This leads us to the ethical question of understanding how algorithms are invading our irrational and instinctive perception of collecting information and reinforcing our ideological positions, instead of bringing us standard and balanced information, in order to contribute to our personal development as human beings. Reflecting to the above, it could also be argued that this management of information is pushing people towards hateful and extremist content, and creating sharper divisions in public opinion, instead of building bridges of mutual understanding and fruitful share of knowledge.

Inside this specific environment and these new technological rules, press companies need to readapt their news content, which in the beginning was not always strategically thought out to be served on Facebook and can still be published. During these years, the stakeholders seem to have gradually understood that content without a strategy, production, and publishing technique can easily get lost in the midst of thousands of social network publications. Hence, the users' impact is evident on the standards sources of information should abide, mainly when it comes to online newspapers and magazines.

It is clear that we live in an information society, in which the creation, usage, distribution, manipulation, and integration of information content is a powerful act. The values of freedom of expression are counterpointing to a certain artificial freedom of thought, by reason of information improved in quantity and sources, but without the quality and necessary exemption for the fulfillment of the duty to inform constructively.

In conclusion, drawing an analogy with the Harry Potter film saga, the algorithm could be compared to the sorting hat, choosing the information that is going to be available in the users' social network feed. As news consumers, we need to filter the relevance of these contents and educate ourselves in how we want to get informed and, most importantly, how do we want to find and reflect on the counterpoints of our positions, so that this evolution can contribute to our personal development.

A Brief Analysis

AN INTRODUCTION TO REGULATORY AND PRIVACY CHALLENGES POSED BY BRAIN COMPUTER INTERFACE SYSTEMS

Lucas Battistello Espindola
LLM Student in Law in a European Global Context at Católica Global School of Law

Ana Rita Santos
LLM Student in Law in Digital Economy at Catolica Global School of Law

Last year, Elon Musk conducted a much-anticipated press conference[1] introducing the recent developments of Neuralink. During a short webcast, a harmless small device introduced into a pig's skull was able to read its brain activity and predict its movements through a wireless brain interface technology. The neurotechnology used is an example of Brain Computer Interface ("BCI") systems - devices that enable a computer or other digital mechanisms to communicate directly with the human mind. As an emerging research field with increasingly economic incentives, the commercialisation of neurotechnology presents itself not only with unlimited potential, but also with unprecedented concerns. For the purposes of this paper, this short article will focus exclusively on some of the legal issues emerging from such debate, with special emphasis on the regulatory and privacy challenges posed by the nature of data obtained through BCI devices.

In order to understand some of the legal concerns of emerging neurotechnology, it is important to understand the specificities of how this technology works. BCI technology is composed of four stages: signal acquisition, information processing, feature extraction and classification with computer interaction. Through these different processes, brain activity is recorded, analyzed and then can be configured as feedback to a computer or translated into a specific command. To be exact, there are several options for invasive and non-invasive brain mapping techniques through the usage of BCI devices. Still, the most relevant method is arguably through Electroencephalogram ("EEG") signals, which uses electrodes to measure electric impulses emitted by a patient's neurons. Such electric signals vary according to different stimuli, rhythms

1 *Further details of Elon Musk's live press conference can be found on Neuralink official website, available online at https://neuralink.com/.*

and frequency of brain activity, which in turn reflect in different data that can be collected through EEG technology.

As for the legal debate itself, the starting point relates to the nature of the data collected through the use of BCI devices. As highlighted in a recent OECD working paper[2], neuroscience as a whole is a relatively unexplored field, and the possibilities and intricacies of data collected through neurotechnology even more so. To be precise, there are characteristics intrinsic to the information collected through BCI that are more complex and do not necessarily fall within the scope of standards of protection and regulatory provisions of legal instruments such as the General Data Protection Regulation (GDPR).[3] Consequently, this scenario raises the question whether current data protection regimes are adequate to protect individuals' rights[4] and, more importantly, if they are suitable for such further unpredictable developments in BCI technology.

The first characteristic is that neurodata is uniquely

2 *OECD, 'OECD Recommendation on Responsible Innovation in Neurotechnology' (OECD, 11 December 2019) <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm> accessed 15 February 2021*

3 *The authors chose to limit most of the scope of their brief analysis to a direct comparison with the GDPR due to the absence of updated legal frameworks that address data collected through neurotechnology specifically. Still, it is arguable that by addressing the core structural principles entrenched within the GDPR, this study can nonetheless provide substantial insights on the data protection field, relevant to the current ongoing debate.*

4 *Neurotechnology poses challenges not only in relation to existing rights, but also introduces a possibility of the creation of new rights, such as Cognitive Liberty, Mental Privacy and Mental Integrity, as well as the right to Psychological Continuity. Still, for the purposes of this article, such topic will not be explored. A further insightful analysis can be found at Marcello Ienca and Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology' [2015] 13(5) Life Sciences, Society and Policy 20*

personal and, different from other types of information, particularly difficult to be dissociated from the individual user they represent. Unlike information such as a user's address, email or browser history, neurodata of brain waves patterns collected by BCI devices will never be identical for any two individuals in any given circumstances.[5] Moreover, with the right external stimuli and brain mapping, these individual neuro patterns can be decoded to reveal sensitive personal information such as one's personal preferences, religion and political beliefs.[6] Consequently, protecting such information through any anonymity or dissociative means regulated through data protection regulatory frameworks becomes a rather challenging (if not impossible task) as neurodata remains a reflection of a subject's individuality.

Secondly, considering the complexity of neurodata, the sheer volume of information that can be collected and the relative unfamiliarity with the possibilities of BCI technology, neurodata is intrinsically complex and the information collected is likely difficult to be restricted in any way of form by the user and, to a certain extent, by the device operator as well.[7] For instance, while it is relatively easy for a user to limit its consent to the information he or she would be providing when accessing a particular website or subscribing to a specific service, the same is not true for a user of a BCI device. This is due to the fact BCI technology reveal a vast amount of complex involuntary information[8] which users might not be able to understand or even be aware of to provide their consent for the acquisition, processing and analysis of data by private companies. Simply put, by its very own nature, neurodata poses challenges to consent and possible restrictions in acquiring information from users.

Consequently, these two characteristics present possible difficulties in applying the current mechanism of data protection framework to neurodata. Most data protection regimes[9] offer protection to data by classifying it as personal or sensitive information[10], which in turn bears many legal consequences as to the

5 *Hema Cr and AdzizulA Osman, 'Single Trial Analysis on EEG Signatures to Identify Individuals' [2010] ( ) 2010 6th International Colloquium on Signal Processing & Its Applications (CSPA) 1*

6 *Ivan Martinovic and others, 'On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces' [2012] ( ) the Proceedings of the 21st USENIX Security Symposium, USENIX <https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final56.pdf> accessed 21 February 2021*

7 *Dara Hallinan and others, 'Neurodata and Neuroprivacy: Data Protection Outdated?' [2014] 12(1) Surveillance & Society 63*

8 *According to the OECD Working Paper, this vast amount of information consists of health information, patters related to specific behavior, involuntary feelings and reactions to external stimuli.*

9 *Authors based their brief assignment on the updated list of countries and their respective level of data protection available at https://www.cnil.fr/en/data-protection-around-the-world*

10 *Hallinan (n 8) 66*

degree in which such information may be processed. Still, the concepts of anonymity and sensitivity cannot be applied – at least not as easily – to neurodata[11]. Similarly, several principles of the GDPR such as purpose specification[12] and data minimization[13] would need to be adapted in order to encompass an increased use of BCI. While current legal systems are not prone to accommodate such technology advancements, it could be suggested a different approach towards rethinking the traditional conceptualization of data for regulatory purposes. For instance, it is argued that the creation of a new regulatory framework can fully encompass the novelty of the neurodata as current frameworks are deficient to do so. Hence, neurodata should be in a special category by itself, since the current regime presents several exceptions that would effectively result in possible privacy violations.

In the field of DNA and cellular data a similar issue has already been explored by the judiciary. In S and Marper v. the United Kingdom[14], the European Court of Human Rights was clear in stating that "the retention of cellular samples and DNA profiles discloses an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 §1 of the Convention". It is arguable that such types of data, by their nature – how they enable identification of individuals and collection of information – are easily comparable with neurodata. As such, similar restrictions to cellular data collection could be imposed into companies operating with neurodata as well.

Hence, given the complexity of the neurodata, it becomes especially hard, as demonstrated above, to ensure compliance and proper protection of information collected through BCI systems. The particularities of this new technology and its challenging consequences are not in a farfetched future. In truth, as this article has briefly shown, the legal concerns, especially in relation to data protection and privacy, are a present issue deserving of further analysis by the international community.

---

11 *ibid 63*

12 *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 2 119/1 (General Data Protection Regulation), art 5(b)*

13 *General Data Protection Regulation, art 5(c).*

14 *S and MARPER v THE UNITED KINGDOM (2008) 1 23*

DOES THE GDPR SENSITIVE DATA REGIME ADEQUATELY PROTECT THE RIGHT TO PRIVACY AND NON-DISCRIMINATION?

Maria Roussi
National Researcher of ELSA Greece
ILRG: Human Rights and Technology

INTRODUCTION

Sensitive data has traditionally been a constitutive element of regulations regarding privacy and personal data. The purpose of this essay is to discuss whether the sensitive data regime of the General Data Protection Regulation effectively protects the rights to privacy and non-discrimination, and to make suggestions to ensure that these human rights are fully safeguarded.

OVERVIEW OF THE REGIME

Personal data is defined in Article 4(1) GDPR as any information that identifies a natural person or makes that person identifiable.[1] However, not all information is equally private or intimate. Therefore, the GDPR's wide scope is counterbalanced by a mechanism which allows the regulation to treat different 'levels' of privacy. Racial and ethnic origin, political opinions, religious and philosophical believes, trade union membership, sex life and sexual orientation as well as genetic, biometric and health data and data relating to criminal convictions and offences are protected by Articles 9 and 10 GDPR. Specifically, the processing of special categories or criminal-related data is banned (albeit as regards criminal-related data only in the private sector), unless there is an additional sensitive legal ground for processing. Furthermore, in its attempt to adopt a more 'risk-based' approach, the GDPR includes discipline provisions, such as requiring controllers and processors to record sensitive data processing or have a data protection officer.[2]

CRITICISMS

The fact that sensitive data are treated more strictly suggests that the EU legislator estimated the risks emanating from their processing to be higher than those from the processing of other types of data.[3] This article will now examine whether these risks are sufficiently avoided, especially in the context of omnipresent digitisation.

Firstly, although maintaining an exhaustive list of sensitive data provides legal certainty, it also causes a risk of overinclusion. In Lindqvist, the ECJ ruled that sensitive data must be interpreted widely.[4] However, the sensitive data regime should function as a corrective to the expansiveness of the GDPR's ambit. Overinclusion could lead to even ordinary processing operations encountering severe legal problems, rather than providing a balance between protection and inoperability. On the other side - of under-inclusion - questions arise as to why some categories have been included and others haven't, such as financial data.[5]

Secondly, the narrow nature of the default bases for processing sensitive categories of data has

1 *See Case C-434/16 Nowak v Data Protection Commissioner ECLI:EU:C:2017:994, para [34]: 'aim of the EU legislature to assign a wide scope to that concept'.*

2 *GDPR Articles 30 and 37.*

3 *Spiros Simitis, 'Revisiting Sensitive Data' (1999), <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680684 5af > last accessed 21 February 2021.*

4 *C-101/01 Lindqvist ECLI:EU:C:2003:596, para [50].*

5 *Karen Mc Cullagh, 'Data Sensitivity: Proposals for Resolving the Conundrum' (2007) Vol. 2, Iss.4, Journal of International Commercial Law and Technology 190, 194.*

meant that 'legislation has had to be created in Member States to provide an explicit legal basis for carrying out otherwise unobjectionable processing'.[6] Consequently, a range of processing operations could be in legal jeopardy, absent the explicit consent of the data subject, such as making arrangements for persons requiring special religious food (religious opinion) or wheelchair access (health data), or the search engine indexing of (public domain) sensitive data which was not made public by the data subject themselves. It also should be recalled that profiling may serve useful and legitimate purposes; for instance, in medicine, datafication of vital signs and treatments could help identify patterns that are relevant to diagnosis or treatment.

Such an issue was examined in GC v CNIL, where the ECJ dealt with requests to de-reference links appearing in Google search results. The personal data contained, inter alia, judicial investigations and information on sentencing for sexual assaults on minors. The right to protection of sensitive data was in conflict with freedom of expression and the right to information. However, there was no adequate derogation for processing of sensitive data in this case. The ECJ held that Google, as the search engine and controller, could self-rely on the substantial public interest derogation in Article 9(2)(g) as a self-executing rule in the absence of national law.[7] This would also trigger the safeguards enshrined in the GDPR. The Court thus found a practical solution to fix the rule-based approach of the regulation.

Thirdly and significantly, an issue arises when it comes to big data and the accumulation of apparently 'innocuous' information that leads to inferences of sensitive attributes;[8] if consumers observe religious food and drink prohibitions or religious holidays, their shopping patterns will reflect this through the presence or absence of certain products. Ethnicity, religion, and sexual preference can be inferred from what individuals

6 *UK Information Commissioner Office, 'The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data'<https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-is-new/public-consultation/2009/pdf/contributions/public_authorities/ico_uk_en.pdf > last accessed 18 February 2021.*

7 *C-136/17 GC and Others v Commission nationale de l'Informatique et des libertes (CNIL) at para [69].*

8 *Frederik Borgesius, 'Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation', (2016), Vol. 32, Computer Law and Security Review 256.*

'like' on Facebook.[9] Therefore, datafication could result in data sets that can reveal sensitive traits for data subjects. In these 'regular data', consent is not required, but the risk associated with processing of sensitive data is still present.[10]

This could jeopardise the right to equal treatment and non-discrimination; the danger with sensitive traits lies in the fact that they tend to perpetuate discriminatory patterns in the data sets. A potential discriminatory effect can be illustrated in the example of risk analysis for loans based on geographical similarity; if the affected areas include racially segregated neighborhoods, such a decision-making process could be a source of indirect discrimination based on a sensitive trait.[11] Of course, Article 22(4) GDPR prohibits automated decision-making and profiling based on sensitive data, unless it is based on explicit consent of the data subject or a substantial public interest is served. However, discriminatory effects can occur even when the data used for profiling is not itself sensitive.

Paradoxically, one technological solution to counteract the manifestation of discriminatory patterns would be to deliberately use sensitive data – however, this would be forbidden by Art 9(1) GDPR. It has been argued that omitting sensitive data may allow indirect discrimination, due to the redlining effect which may happen when legitimate variables (such as a zip-code) are correlated with sensitive characteristics, and thus may act as a proxy for the sensitive characteristics (such as race).[12] Consequently, a better strategy might be to learn a model on data including the sensitive variable, then remove the component with the sensitive variable, and replace it by a constant that does not depend on the sensitive variable.

SUGGESTIONS

The consent requirement of Article 9 GDPR suggests that the regulation aims to strengthen data subject participation in the processing of their sensitive data, thus encouraging a discourse-based management strategy, consisting of building up consciousness and initiating collective efforts. Indeed, risk management should strike a balance between precaution-based and discourse-based measures. Precaution alone may be effective in preventing adverse effects but could also make the benefits of datafication unattainable.[13]

Furthermore, flexibility would be increased if the list of special categories became open-ended. In addition, a general-criteria test could be introduced, which would follow a context-based approach and evaluate the risk of processing under the specific circumstances.[14] Personal data could be considered sensitive, depending on contextual information such as the interests of the data controller, the recipients of the data, the aims of the processing, and its possible consequences. It should be recalled that the EU framework already requires, in the case of processing of special categories of data on a large scale, impact assessments[15] and potentially prior consultation with a Data Protection Authority, to ensure the safeguarding of data that poses a high risk because of the context of the processing.

Finally, the GDPR's introduction of pseudonymization and its greater emphasis on anonymization could provide opportunities for data controllers to use personal data in more innovative ways.[16] Once data is anonymised and individuals are no longer identifiable, the data will not fall within the scope of the GDPR and it becomes easier to use. On the other hand, pseudonymisation techniques will not exempt controllers from the ambit of GDPR altogether. They do however help controllers meet their data protection obligations, particularly the principles of 'data minimisation' and 'storage limitation' and processing for research purposes for which 'appropriate safeguards' are required. Therefore, from a legal perspective, it is allowed to create models on data, including sensitive data that is anonymized, that are nondiscriminatory. Of course, the Article 29 Working Party observes the risks of insufficient anonymization, such as linkability (a known sensitive trait of a particular data subject can be linked to supposedly anonymized data from another context), and thus anonymization should also be used with caution.[17]

---

9 M Kosinski, D Stillwell, T Graepel 'Private traits and attributes are predictable from digital records of human behaviour', (2013), 110(15) Proc Natl Acad Sci 5802, 5805.
10 Michiel Rhoen and QY Feng, 'Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science', (2018), Vol. 8(2), International Data Privacy Law 140.
11 Ibid 147.
12 Žliobait and Custers 'Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models', (2016), Vol. 24(2), Artificial Intelligence and Law 183.
13 Rhoen and Feng (n 10), 159.
14 Simitis (n 3).
15 GDPR Art 35.
16 Žliobait and Custers (n 12). See also Recitals 26 and 28 GDPR.
17 A29 Working Party 'Opinion 05/2014 on Anonymisation Technique',

A new infringement of your privacy?

THE UNKNOWN POWER OF DEEPFAKES

Mariana Fernandes
Member of ELSA Universidade do Minho

Were you ever bored and decided to put your face in Nicolas Cage's body using a random app from your App Store? Have you ever seen a video of Barack Obama that looked somewhat strange? Then you might already be aware of deepfakes.

This new enigmatic problem is what Jeremy Kahn, a tech reporter from Bloomberg, calls "fake news on steroids", a nomination quite true to the danger and risks that it might bring. Deepfakes are, therefore, synthetic media that can serve multiple purposes. In this process, any original video can be morphed and create a new "reality" which can lead the viewer to be fooled and believe this new product and its content. Deepfakes have been around since 1990, although its new surge in popularity is what concerns the specialists of this field. With the advance in technology and new generations being able to understand software and technology easily, deepfakes have been normalised. The software in charge of making this synthetic media has, throughout the years, become cheaper and easier to learn, making the process of creating deepfakes easier and quicker, allowing it, and its intentions, to spread widely.

Although this new software might seem amusing and entertaining, in it lays a dangerous path to the violation of our right to privacy.

Privacy, and the right of our own image, is a fundamental right recognised by Article 12 of the Universal Declaration of Human Rights, which states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

As a result, it's safe to say that it's in our human nature to be in control of our image and perception. The mere thought of someone using our name and image without our consent and controlling it has been one of the great fears of Man, trickling it into battles and dishonor to an extent. Our image is deeply connected to us as human beings and to our role in society.

Deepfakes can be harmless and engaging, this software has been used to bring back memories of a not so distant past, for example, the Illinois Holocaust Museum and Education Center used deepfake software to create an interactive interview between the visitor of the museum and a Holocaust survivor in order to hear, first-hand, their story.[1] Nevertheless, this reflects a minor percentage of the usage of deepfakes.

The negative consequences of synthetic media are much more prevalent, going from the distortion of the face and voice of famous politicians[2] to the use of famous female actresses faces in pornography

1 *"Take a Stand Center «Illinois Holocaust Museum and Education Center" (Ilholocaustmuseum.org2020) <https://www.ilholocaustmuseum.org/tas/> accessed February 17, 2021*
2 *deepfakes, "Trump | Deepfakes Replacement" <https://www.youtube.com/watch?v=hoc2RISoLWU&feature=emb_logo> accessed February 18, 2021*

without their consent. On a much closer level, the possibility of someone using our face and name to form deepfakes is more real every passing day, and with the endless possibilities that the internet has to offer, it's fair to say that the unlawful and insincere use of our image can lead to various negative consequences in our social and professional life. Thus, it is understandable the dangers and immorality that deepfakes can bear not only to the citizen, but also to the State.

In a world in which every image and video can be manipulated, what should the people think? Can reality be faked? Future might be uncertain in relation to deepfakes, leaving it up to the people to stay informed and protect their own right of privacy until the State finds a suitable way to protect not only their citizens, but also themselves.[3]

Regarding this matter, and in recent news, the European Union has briefly regulated deepfakes in the new Digital Services Act[4], as well as the new Europol's report which states the risks of this synthetic media and alerts to this new rising global problem.[5]

Lastly, a world in which deepfakes stay in the legal grey area can lead to an uncertain and critical spread of fake news and the violation of our privacy. Our fundamental right to privacy cannot coexist with the negative and disastrous aspects of deepfakes, and therefore we must challenge our State and representative politicians to take action now and protect us from a bizarre reality which can be altered by whomever seems fit.

3 Author Nina Schick refers this idea in Nina Schick, Deepfakes: the coming infocalypse (2020)
4 "The Digital Services Act: Ensuring a Safe and Accountable Online Environment" (European Commission2021) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed February 18, 2021
5 Trend Micro Research; United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol's European Cybercrime Centre (EC3), Malicious Uses and Abuses of Artificial Intelligence (2020)

ClickMeeting

Video conferencing, online meetings, and webinar software

to bring your students, customers, and team members together.

Product demos & marketing

Buying decisions start with education. Showcase your product. Share your insights. Sell.

Online courses & training sessions

Share your knowledge with online courses and training sessions. Teach your students from anywhere.

Online business meetings & collaboration

Run your projects smoothly. Meet and collaboration on the move

Huge online events

Scale up your webinars and reach thousands of people across the globe.

clickmeeting.com | sales@clickmeeting.com

How free speech, the presumption of innocence and the in dubio pro reo principle coexist in the digital era

IS THE INTERNET COMPROMISING THE RIGHT TO A FAIR TRIAL?

Vasiliki Monika Pontikidou
Member of ELSA Thessaloniki

In the 18th century, jurist and judge William Blackstone coined the famous phrase known as the Blackstone Formulation: 'Better that ten guilty persons escape than that one innocent suffer.' This phrase embodies the principle that courts should err on the side of innocence rather than convict a suspect when their guilt is not proven beyond a reasonable doubt (in dubio pro reo, 'in doubt for the accused'). Along with the presumption of innocence, they form the two pillars that support the right to a fair trial. From the Babylonian Code of Hammurabi to ancient Greece and the Roman law,[1] legal texts and traditions recognise the right of the defendant to be considered innocent until found guilty in a court of law. Today, this principle is protected by the Charter of Fundamental Human Rights, the European Convention on Human Rights and many other international conventions.

The aforementioned principles are of great importance in penal cases where the verdict is decided by a jury. In fact, jury systems were created based on the belief that their verdict serves as a 'veritatis dictum', a fair and appropriate decision founded on our common sense of justice. Upon the beginning of a jury trial, jurors are given clear instructions to decide based only on the facts and evidence presented at trial. However, it is increasingly easy to form subjective opinions and be influenced by extra-evidentiary factors, such as stereotypes, biases and heuristics[2], even unconsciously. Especially in cases of high public interest, characterised by a constant barrage of news and opinions regarding every aspect of the case, from

1 *A. Deegan, 'The Internet is Changing the Presumption of Innocence' (Local Umbrella News, 18 July 2019) <https://localumbrellanews.com/andrew-deegan-attorney-at-law-the-internet-is-changing-the-presumption-of-innocence/> accessed 22 February 2021*

2 *A heuristic is a mental shortcut that allows people to solve problems and make judgments quickly and efficiently, but which can also lead to cognitive biases.*

the private life of the accused to the reliability of expert testimonies, the question seems more prominent than ever: How can we ensure a just and impartial jury decision in the digital age without limiting free speech and the freedom of media?

In today's saturated media culture, the Internet and social media have brought to the surface the new 'court of public opinion'. The most prominent example: the acquittal of Casey Anthony; greeted by intense public outrage after a highly publicised trial and named by Time magazine as the 'social media trial of the century'.[3] There is ample research proving that media exposure describing the defendant in a negative light can cause jurors to view them more harshly, and result in more guilty verdicts compared to jurors not exposed to such coverage.[4]

As the press and television give way to the Internet, this risk is magnified. More specifically, the potential misuse of social media by jurors during trials is identified as the biggest challenge that social media pose to courts.[5] Reuters Legal has found that at least 90 verdicts in the US between 1999 and 2010 were challenged due to juror Internet misconduct.[6] From researching legal terms online to one juror posting a poll on Facebook asking her followers for help on which verdict to decide, it is more than clear that the arising threats to legal systems worldwide are multiplied.

Under these conditions, juror misuse of the Internet, as well as intense media coverage, can have profound effects on the way that jurors reach their decisions and that justice overall is served. They can lead to polarisation, pervasion of biases and jury contamination, they reinforce negative attitudes of the public towards the defendant through criminal labeling and in the end, substitute opinion for fact, making it increasingly difficult to reach a fair, unanimous verdict. Nevertheless, the press and media are fundamental pillars of democracy and are protected on a constitutional and international level. The above threats do not mean that the Internet and social media are inherently 'evil', nor that the rise of the Internet and jury trials are a priori mutually exclusive.

Rather, examining them can remind us that, if these challenges are eliminated, these seemingly 'opposing forces' can meet. Both freedom of speech online and jury systems serve the same purpose at their core: to be used against the miscarriage of justice, to encourage positive changes in policy and behavior and to revive the public's trust to a justice system that ensures fair and equal treatment for all.

3 J.Cloud, 'How the Casey Anthony Murder Case Became the Social-Media Trial of the Century' (TIME, 16 June 2011) <http://content.time.com/time/nation/article/0,8599,2077969-2,00.html> accessed 22 February 2021

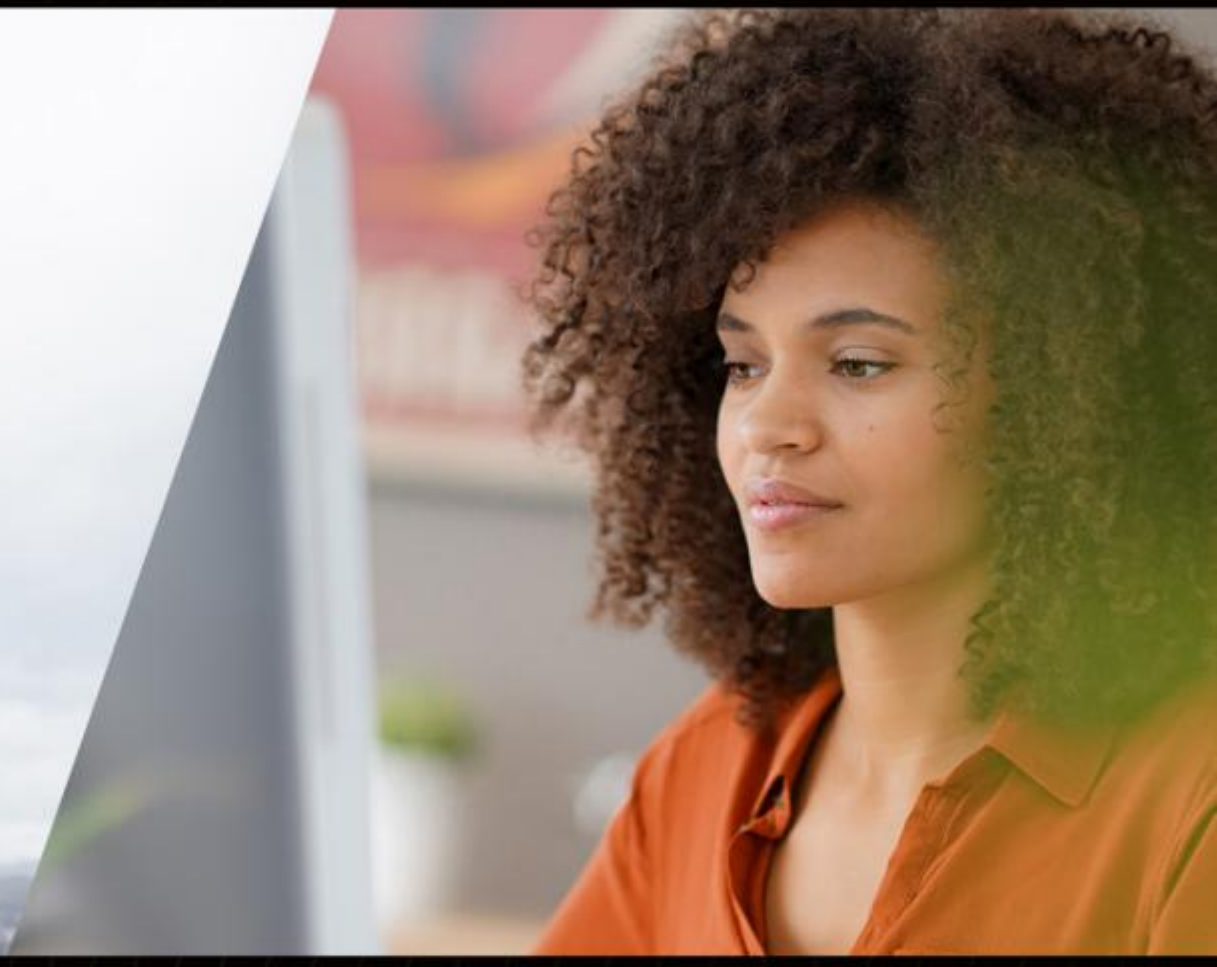
4 C. Ruva and C. McEvoy, 'Negative and Positive Pretrial Publicity Affect Juror Memory and Decision Making' [2008] 14(3) Journal of Experimental Psychology Applied

5 J. Johnston and others, 'Juries And Social Media, A Report Prepared For The Victorian Department Of Justice' <https://www.researchgate.net/publication/275037791_Juries_and_Social_Media_A_report_prepared_for_the_Victorian_Department_of_Justice> accessed 22 February 2021.

6 B. Grow, 'As jurors go online, US trials go off track' (Reuters, 8 December 2010) <https://www.reuters.com/article/us-internet-jurors-idUSTRE6B74Z820101208> accessed 22 February 2021

FAST-TRACK
YOUR CAREER NOW

ELSA's Traineeship Programme, STEP offers hundreds of internship opportunities all around the world or remotely from the comfort of your home.



Applications will stay open until the 14th of May.
Visit step.elsa.org now!

STEP
TRAINEESHIPS
STEP.ELSA.ORG

elsa
The European Law Students' Association

THE
JOHN H. JACKSON
MOOT COURT COMPETITION

elsa
The European Law Students' Association

WORLD TRADE
ORGANIZATION
TECHNICAL SUPPORTER

PARTICIPANTS OF THE 19TH EDITION OF THE JOHN H. JACKSON MOOT COURT COMPETITION

ELSA IS ORGANISING THE BIGGEST MOOT COURT COMPETITION ON INTERNATIONAL TRADE LAW, WITH THE TECHNICAL SUPPORT OF THE WORLD TRADE ORGANISATION (WTO).

DATA MASKING, A CHALLENGING BALANCE

Giacomo Benaglia
Member of ELSA Bologna

Recent years have seen the consistent growth in attention towards technical solutions aimed at safeguarding the fundamental right to privacy, in compliance with a number of instruments enshrining it, both in an international and regional landscape, most notably, in the European context, the GDPR. Such solutions, however, are often faced with the challenging need to harmonise and conjugate the protection of such a crucial right with present capabilities at the same time to effectively pursue different objectives in the use of these technologies, whether that is, for example, health research, statistical analysis in the banking industry or the management of human resources within a company.

In such situations, 'data masking' can represent a valuable asset to be deployed in the protection of individual privacy, realising the crucial balance between the intrinsic and ever-growing need for data required by novel technologies, and the need to protect, at the same time, the sensitive information of the subjects involved. Also referred to as data obfuscation, pseudonymisation or a variety of synonyms often corresponding to subtle differences, data masking can generally be defined as a technique of altering certain data values by substituting them with fictitious ones, while at the same time maintaining their original format.[1] This allows interested parties to utilise the masked data regardless of the process they have just undergone, while the sensitivity of the information has, on the other hand, still been preserved.[2] The data appears in fact, at this stage, to still be coherent and realistic, however all the elements that allow for the identifying of a subject or individual by their data have been removed.

This process ought to be distinguished from encryption, as both practices are based on the concealing of data to ensure the protection of privacy. While the latter is in fact a reversible process, this is not the case with data masking, as the transformation does not allow for a successive recovery of the masked values. In addition,

1 *Hush Hush, 'Data Masking Definition', <https://mask-me.net/datamaskingwiki/wiki/26/data-masking-definition> accessed 15 February 2021*

2 *Securosis, 'Understanding and Selecting Data Masking Solutions: Creating Secure and Useful Data' (10 August 2012), 2, 6 <https://securosis.com/assets/library/reports/Understanding-Masking_FinalMaster_V3.pdf> accessed 15 February 2021.*

encrypted data is not directly readable without first being decrypted with the use of the proper key, in contrast to masked data, which will purposely lose their original values.[3] As a result, the respective fields of application tend to differ slightly, with data masking appearing particularly suited towards testing and analysis applications, as privacy protection will not only be directed towards potential external breaches but also towards subjects directly processing and utilising the data.[4]

Data masking procedures are carried out by specific software and offer a wide variety of approaches, ranging from the reorganisation of the same values within data in a random order, for example numbers, to the substitution of real values with a fictional set of realistic ones, mostly in case of words.[5] Despite a number of different solutions, a common and fundamental characteristic is found in the usability and coherence of the data emerging from the masking procedure. A typical example, in this sense, can be afforded by the substitution of personal identifying information such as the name and surname of an individual, or their address with a fictitious one, while maintaining other values associated with the data. For instance, in order to securely process medical data or card payment details, insurance-related information, user data linked to the use and enjoyment of products and services provided online.[6]

A relevant distinction can also be outlined between the so-called 'static' and more recently developed 'dynamic' practices of data masking. While in the first case, data is permanently altered, in the latter, the process of transformation takes place during the transfer, the movement of such data towards, for example, an external user with fewer authorisations trying to access them, which leaves the original source intact. Each solution suits different needs. For example, as static data masking allows for stronger protection of sensitive information in hypothetical data breaches, the dynamic approach affords more flexibility for the subjects implementing it in determining the variable

3 ibid 6; Nikhil Ranjan, 'Data Masking: What It Is, Techniques and Examples' (Informatica Blog, 16 September 2015), <https://blogs.informatica.com/2015/09/16/differences-between-encryption-and-masking/> accessed 17 February 2021.

4 MENTIS INC, 'Encryption vs. Tokenization vs. Masking' (11 December 2019), <https://medium.com/@mentisinc/encryption-vs-tokenization-vs-masking-f69df9534fea> accessed 17 February 2021; Hush Hush, 'Encryption Vs Data Masking', <https://mask-me.net/datamaskingwiki/wiki/195/encryption-vs-data-masking> accessed 16 February 2021; Securosis, 'Understanding and Selecting Data Masking Solutions: Creating Secure and Useful Data' (10 August 2012), 3 <https://securosis.com/assets/library/reports/UnderstandingMasking_FinalMaster_V3.pdf> accessed 15 February 2021.

5 Imperva, 'Data Masking', <https://www.imperva.com/learn/data-security/data-masking/> accessed 16 February 2021; Securosis, 'Understanding and Selecting Data Masking Solutions: Creating Secure and Useful Data' (10 August 2012), 2 <https://securosis.com/assets/library/reports/UnderstandingMasking_FinalMaster_V3.pdf> accessed 15 February 2021.

6 AI Multiple, 'Data Masking: What it is, how it works, types & best practices' (13 November 2020), <https://research.aimultiple.com/data-masking/> accessed 18 February 2021; Anh T. Pham, Shalini Ghosh, Vinod Yegneswaran, 'Data Masking with Privacy Guarantees' (2019), 1 <https://arxiv.org/pdf/1901.02185.pdf> accessed 21 February 2021; Samadhan Kadam, 'Data Masking: Concept, Tools, Masking polices & Healthcare Data Masking' (21 June 2019), <https://medium.com/petabytz/data-masking-concept-tools-masking-polices-healthcare-data-masking-c28ca03a30a> accessed 18 February 2021.

amount of information they may wish to disclose.[7]

Regardless of the different nuances in the approach or even the technique applied, data masking emerges as a relevant solution for the vindication of crucial privacy rights. These would be in line with, for example, the Revised Payment Services Directive or, more prominently, a consistent number of provisions of the GDPR. Regarding the latter, the most relevant articles appear to be the 6, 25 and 32, all of which provide for the adoption and implementation of proper technical measures of protection, such as encryption or the pseudonymisation of personal data. It is worth highlighting that these articles, as well as article 40 and 89, all explicitly refer to practices defined as 'pseudonymisation', such as the ones outlined. Furthermore, in terms of the above-mentioned articles, it is essential to add the fifth article of the regulation, which enshrines an underlying principle that is fundamental to the whole matter at hand. It is also particularly relevant in outlining and understanding the scope of data masking, the principle of accountability and, most of all, the principle of data minimisation.[8] Article 5-par.c states that the processing of personal data shall be limited to what is necessary for the purpose of such processing, therefore giving effect to the required fundamental equilibrium between the right to privacy and commercial action or different objectives pursued.[9]

In conclusion, in a context in which constant developments in technology often raise concerns regarding their impact on fundamental rights, solutions such as data masking show how technology can present itself as an invaluable and effective tool to enforce human rights protection.

7 *Steve Pomroy, 'Static Versus Dynamic Data Masking' (10 July 2017), <https://www.imperva.com/blog/static-versus-dynamic-data-masking/> accessed 18 February 2021; Microsoft, 'Dynamic Data Masking' (5 February 2019), <https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver15> accessed 18 February 2021.*

8 *AI Multiple, 'Data Masking: What it is, how it works, types & best practices' (13 November 2020), <https://research.aimultiple.com/data-masking/> accessed 18 February 2021; Dario Colombo, 'Data masking, soluzione per adempiere a GDPR' (27 November 2017), <https://www.01net.it/data-masking-soluzione-gdpr/> accessed 19 February 2021; Alessandro Ronchi, 'Data masking e GDPR' (23 May 2018), <https://ronchilegal.eu/2018/05/23/data-masking-gdpr/> accessed 19 February 2021.*

9 *EU General Data Protection Regulation (GDPR): 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.*

Article 17 of the GDPR and the Right to be Forgotten

RIGHT TO BE FORGOTTEN

Danai Kyriakantonaki
Member of ELSA Komotini

The term "Right to be Forgotten" or "Right to Erasure" is used in the context of privacy and data protection law. According to the "Right to Be Forgotten", which is provided in Article 17 of the proposed General Data Protection Regulation, individuals are given a means to oppose enduring the digital memory of the Web.[1] The assertion of the right to have a subject's own data erased is particularly crucial for the efficient application of data protection principles, and notably the principle of data minimisation. According to this principle, personal data must be strictly limited to what is necessary for the purposes for which that data is processed.[2] In addition, Modernised Convention 108 explicitly recognises that every individual has a right to the erasure of inaccurate, false or unlawfully processed data.[3]

In particular, under EU law, Article 17 of the GDPR gives effect to data subjects' requests to have data erased or deleted and no longer processed. The right to have one's personal data erased without undue delay applies where:

- the personal data is no longer necessary regarding the purposes for which they were collected or otherwise processed;
- the data subject withdraws the 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 has been unlawfully processed;
- the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data has been collected concerning the offer of information society services to children pursuant to Article 8 of the GDPR.

Further analysis regarding the last bullet should be made. According to this provision, the protection of the personal data of children is enforced, as it grants a right to erasure for data processing in relation to information security services based on a child's consent. The cause of this rule is affiliated with the fact that a child might not be fully aware of the risks involved in data processing, and as a result, expects it to be removed in the future. The exercise of this right is independent of the fact that the data subject may no longer be a child.[4]

The role of time in the evaluation of data

As several studies point out, the Right to be Forgotten "is based on the autonomy of an individual becoming a right holder in respect of personal information on a

1 *Serge Gutwirth-Ronald Leenes-Paul de Hert, Reforming European Data Protection Law, Law, Governance and Technology Series 20, 2015*
2 *Handbook on European data protection law, 2018*
3 *Modernised Convention 108, Art. 9 (1) (e).*
4 *Worms, in: Wolff/Brink, BeckOK, Art. 17 (2016) , recs. 50–53.*

time scale; the longer the origin of the information goes back, the more likely personal interests prevail over public interests."[5] There are two characteristic cases that are strongly related to this theory, Segerstedt-Wiberg and Others v. Sweden[6] and Brunet v. France.[7]

In Segerstedt-Wiberg and Others v. Sweden, the applicants had been connected to certain liberal and communist political parties. In spite of the storage of the data at issue having a legal basis and pursuing a legitimate aim, in respect of some of the applicants, the ECtHR established that the continued retention of the data was an unreasonable interference in their private lives. For instance, in the case of one applicant, the authorities retained information that, in 1969, he had allegedly advocated violent resistance to police control during demonstrations. As it was proved, this information could not have any relevant national security interest, particularly given its historical nature. Eventually, the Court found a breach of Article 8 of the ECHR regarding four of the five applicants as to the lack of relevance of the continued storage of their data, considering the lengthy time lapse since the applicants' alleged actions.

In Brunet v. France, the applicants denounced the storage of their personal data in a police database that contained information on convicted persons, accused persons and victims. The criminal proceedings against the applicant had been discontinued, nevertheless his details appeared in the database. Examining this case, the ECtHR held that there had been a violation of Article 8 of the ECHR. In reaching its conclusion, the Court considered that, in practice, there was no possibility for the applicant to have his personal data deleted from the database, although it was intrusive to his privacy, given the fact that details of his identity and personality were incorporated. Furthermore, it indicated that the retention period for personal records in the database, which amounted to 20 years, was unreasonably lengthy, particularly since the applicant had never been convicted by any court.

Exceptions from the data subject's right to be forgotten

The nature of the information in question is a particularly crucial component. If the information relates to the private life of the individual, and there is no public interest in the availability of the information, data protection and privacy would outweigh the right of the general public to have access to the information. On the contrary, if the data subject is a public figure, or if the information is of such a nature as to justify its availability to the general public, then the general public's predominant interest in having access to the information may advocate the interference with the data subject's fundamental rights to data protection and privacy.[8]

Article 17 Sec. 3 lits. a–e of GDPR provides for exceptions from the data subject's right to erasure to the extent that processing is necessary for the following:

- Exercising the right of freedom of expression and information: This right cannot only be invoked by the press but also by any entity.[9] It should be underlined that the distinction between personal data and opinion can be challenging, where an opinion is formed on personal data. In such a case, it needs to be balanced out whether the underlying personal data is still necessary for forming an opinion. The older the personal data is, the more improbable is their necessity for forming an opinion, as it was analysed in a previous chapter.[10]

- Compliance with a legal obligation of the controller requiring processing by EU or EU Member State law/ the performance of a task carried out in the public interest/the exercise of official authority vested in the controller: under this exception, a legal requirement of processing overrides the interest of the data subject to achieve an erasure of its personal data. This exception is commonly, inter alia, arisen from national commercial or tax law.[11]

- Reasons of public interest in the area of public health: this exception is to be interpreted in accordance with Art. 9Sec. 2 lits. h, I and Sec. 3 GDPR.

- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as an erasure of the personal data would render impossible or seriously impair the achievement of the objectives of such processing: the scope of application

5 *Weber, R. (2011). The Right to be Forgotten: More than a Pandora's Box? In2 JIPITEC120, 121. Retrieved from http://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf.*
6 *ECtHR,Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006, paras. 89 and 90*
7 *ECtHR,Brunet v. France, No. 21010/10, 18 September 2014*
8 *Handbook on European data protection law, 2018*
9 *Kamlah, in: Plath, BDSG/DSGVO, Art.17 (2016), rec.17; Worms, in: Wolff/Brink, BeckOK, Art.17 (2016), rec. 81.*
10 *ECJ, ruling of 13 May 2014, Google Spain, C-131/12, rec. 93; Kamlah, in: Plath, BDSG/DSGVO, Art. 17 (2016), rec. 17*
11 *Laue/Nink/Kremer, Datenschutzrecht, Rechte der betroffenen Person (2016), rec. 50*

of the exception as to research purposes is ambiguous as the necessity of personal data for attaining research findings can often only be determined after the research work has been completed.

•Establishment, exercise or defence of legal claims: This exception applies to data that might become relevant for (future) legal claims of the controller and, thus, where its erasure would prevent or complicate the controller's assertion of rights. A right to erasure should be excluded where the controller and the data subject are involved in ongoing or impending legal proceedings.

A balancing of interests on a case-by-case basis is fundamental, because the presence of any of these exceptions requires that processing is necessary for the enumerated reasons. The controller carries the risk for its evaluation of the case, as well as the burden of proof for the existence of such an exception.[12]

In Camera di Commercio di Lecce v. Manni[13], the CJEU had to examine whether an individual was entitled to invoke his right to obtain the erasure of his personal data published in a Public Registry of Companies, once his company ceased to exist. Mr Manni had requested that the Lecce Chamber of Commerce delete his personal data from that registry, as he had discovered that potential clients would consult the registry and figure out that he had previously been the administrator of a company declared bankrupt more than a decade earlier. The applicant supposed that this information would deter potential clients and as a result, would have a negative reflection on his professional future. The CJEU held that "it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary." Due to the legitimate aim of the disclosure and the difficulties in establishing a period at the end of which the personal data could be erased without harming the interests of third parties, the CJEU concluded that EU data protection rules do not guarantee the right to be forgotten for persons in Mr Manni's situation.

Data of the Deceased

Last but not least, it should be examined whether the Right to be Forgotten can be applied to the deceased. In most legal regimes, the data relating to the deceased is not personal data in the strict sense of the word, although the virtually permanent data of the deceased may revolve in web-based services for a long time. In the case of the deceased, only the surviving relatives are able to enforce the right to be forgotten. In such a case, the main aim is not the protection of personal data, but the protection against the injury to the memory of a deceased person. It should be noted that data relating to the deceased may also relate to the surviving relatives, and hence the decision whether or not to erase the data depends on more factors than just the interest of the deceased.[14]

12 *Paul Voigt-Axel von dem Bussche,The EU General Data Protection Regulation (GDPR), 2017*

13 *CJEU, C-398/15,Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 9 March 2017*

14 *Serge Gutwirth-Ronald Leenes-Paul de Hert, Reforming European Data Protection Law, Law, Governance and Technology Series 20, 2015*

The case of Gorlov and Others v. Russia

VIDEO SURVEILLANCE OF DETAINEES IN THEIR CELLS ?

Anastasios Malidelis
Member of ELSA Komotini

While the essential object of Article 8 is to protect the individual against arbitrary action by the public authorities,[1] it does not merely compel the State to abstain from such interference, but also may impose positive obligations inherent to an effective respect for private life.[2] The ECtHR has ruled that the private life is a broad concept which is incapable of exhaustive definition.[3] This generous approach has allowed the case-law to develop in line with technological developments.

The Court dealt with this technological development, and specifically with the videotaping of the detainees' cells in case of Gorlov and Others v. Russia[4]:

The applicants in the case of Gorlov and Others v. Russia complained, in particular, that constant surveillance of their cells, at times by female guards, via closed-circuit television cameras had violated their right to respect for their private life, as guaranteed by Article 8 of the Convention. In the cells, there were cameras installed above the door at ceiling level, in such a manner that the entire cell was clearly visible, including the bed. The applicants argued that they had remained exposed at all times, including when changing their underwear or relieving themselves. In the cells there was a CCTV camera installed above the door, at ceiling level, in such a manner that the entire cell was clearly visible, including the bed. Nevertheless, the toilet was located directly below the camera and was almost entirely hidden from the camera's view by a shield. As a result, it was proved that the toilet and sleeping place were outside the camera's field of view. The applicants stressed that it had been strictly prohibited to hinder surveillance by covering the CCTV camera, even for a short while, for instance, when changing underwear or using the toilet. The applicants also disputed that such an intrusive measure as permanent video surveillance of all cells was necessary for ensuring security and control and maintaining order.

The ECtHR reiterated its consistent case-law that prisoners generally continued to enjoy all the fundamental rights and freedoms guaranteed under the Convention, except for the right to liberty, where lawfully imposed detention expressly fell within the

1 *indicatively, Kroon v. the Netherlands §31*
2 *Helmut Satzger, Internationales und Europäisches Strafrecht, 2020, Baden-Baden, 9.Auflage, NomosLehrbuch, S. 312, Lozovyye v. Russia §36, B□rbulescu v. Romania §§108-111*
3 *indicatively, Costello-Roberts v. the United Kingdom §36, Niemietz v. Germany §29, Pretty v. the United Kingdom § 61; Peck v. the United Kingdom, § 57, Carvalho Pinto de Sousa Morais v. Portugal 25.7.2017, n. 17484/15 §35*
4 *see also Izmestger v. Russia, Riina v. Italy*

scope of Article 5.[5]

The Court concluded that although the Court is prepared to accept, having regard to the ordinary and reasonable requirements of detention, that it may be necessary to monitor certain areas of pre-trial and penal institutions, or certain detainees on a permanent basis, including by a CCTV system, it finds that the existing legal framework in Russia cannot be regarded as being sufficiently clear, precise and detailed to have afforded appropriate protection against arbitrary interference by the authorities with the applicants' right to respect for their private life".

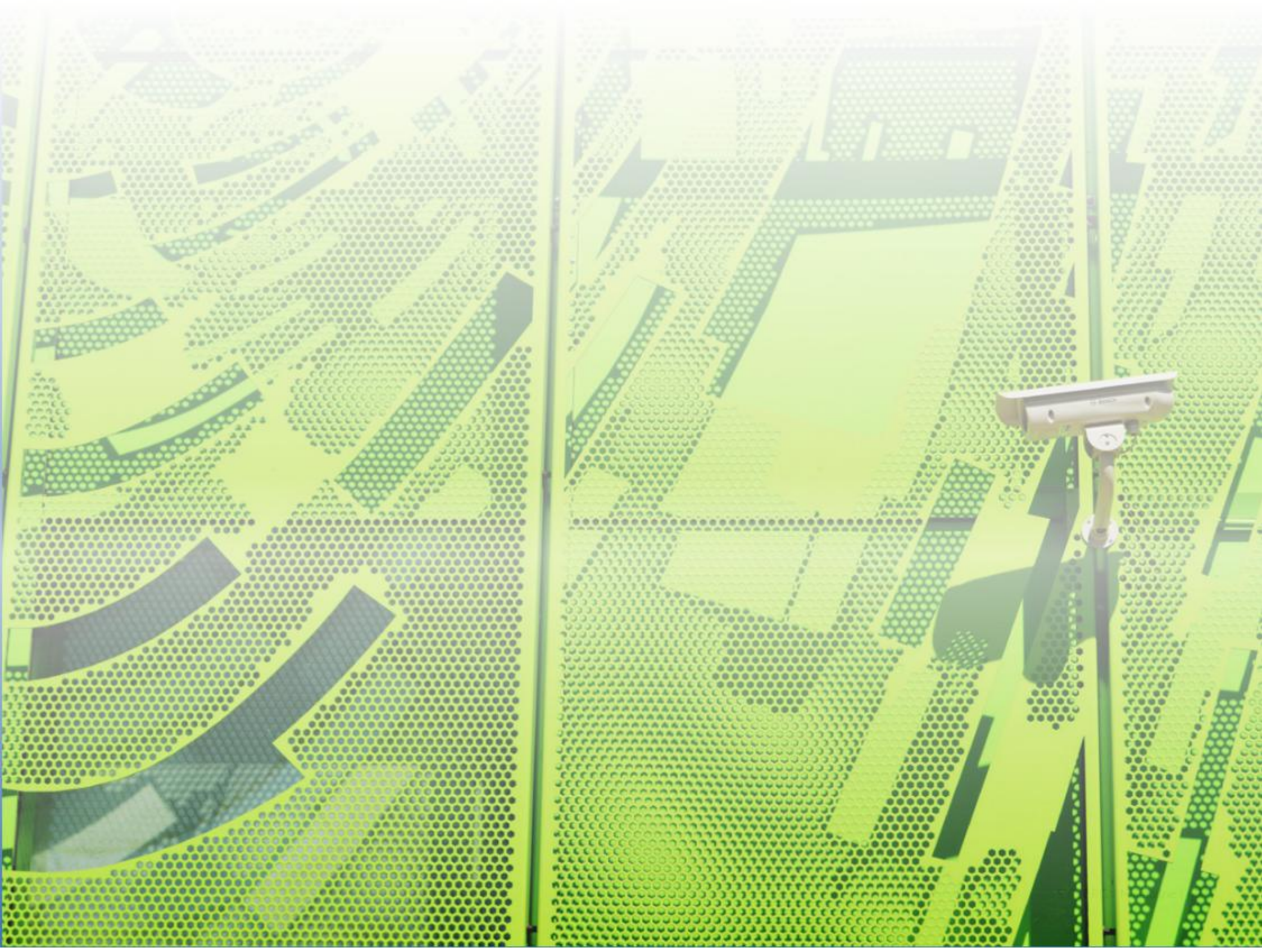
It becomes so clear that permanent video surveillance of detainees in their cells was not in accordance with the law as required by Article 8 § 2 of the Convention.

The Court, in protecting one of the most precious of Human Rights, ruled in the case of Antović and Mirković v. Montenegro §44 that video surveillance of employees at their workplace, whether covert or not, constituted a considerable intrusion into their private life, and that the use of applicants' personal data by audiovisual media without their consent violates Article 8, especially in the case of an accused.[6]

The case law of the ECtHR therefore takes into account the rapid technological development and the intervention that the latter attempts in the personal sphere of the individual. Big Brother is forbidden to supervise even those who have been deprived of the most precious of Human Rights.

5 *Hirst v. the United Kingdom no. 2 § 69*

6 *see Khmel v. Russia § 40, Sciacca v. Italy §§ 29-31, Toma v. Romania §§ 90-93, Khuzhin and Others v. Russia §§ 115-118*



TikTok and the right to privacy

SHOULD I POST THIS?

Eleni Pesmatzoglou
Member of ELSA Thessaloniki

2020. The year considered one of the darkest in the 21st century due to the pandemic crisis. The year when the importance of social media and technology was realised, even by its opponents. Hardly one can deny the fact that digital technology delivers many benefits. Its value for human rights and development is enormous. Apart from the fact that one can empower, inform, investigate, protest and openly express their opinion, during this pandemic crisis, the ability to communicate in an audiovisual way was considered a blessing to our society. In order to fill the endless hours of boredom, there were many who resorted to applications such as TikTok and Snapchat. Even before the pandemic crisis, researches estimated that almost half of the world's population was online every day. The onset of the coronavirus pandemic saw a sustained surge in online activity across the world, with a 18% percent increase in in-home data usage.[1]

Since data collection is already taking place on an industrial scale, it would be unwise to ignore the fact that the digital revolution poses a major global human rights issue. Its indisputable advantages do not negate the fact that, at the same time, the existing privacy legislation in this digital era is violated on a daily basis.

The right to privacy is a fundamental human right recognised in the Universal Declaration of Human Rights (UDHR) and whose protection is enshrined in various pieces of legislation. It is addressed in the constitutions of most countries, and its protection is achieved through the rules of both International and European law. Most notably, Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which is ratified by 173 States and also provides protection from arbitrary or unlawful interferences with the right to privacy; the UN Resolution 68/167, passed by the UN General Assembly in 2013 and clarifies all safeguards for an individual's right to privacy apply while online; the EU Charter of Fundamental Rights, which stipulates that EU citizens have the right to protect their personal data and the General Data Protection Regulation (GDPR)/ Regulation (EU) 2016/679, stipulating the protection of natural persons with regard to the processing of personal data and the free movement of such data.

Examining the TikTok application more closely, one can easily notice that it is an application committing various infringements in the protection of personal data. TikTok is an application owned by the Chinese private company ByteDance, which enables users to create and share short videos, to which they can add music and other special effects.

Already, back in 2019, it was under investigation in the United Kingdom because of the way it collects and uses the personal information of children and teen users, both categories in which it is extremely popular.[2]

During 2020, there had been numerous complaints

1 *Jessica Clement, "Coronavirus: impact on online usage in the U.S. - Statistics & Facts", (STATISTA, 8 January 2021), <https://www.statista.com/topics/6241/coronavirus-impact-on-online-usage-in-the-us/> accessed 15 February 2021.*

2 *Alex Hern, "Tik Tok under investigation over child data use", (The Guardian, 2 July 2019), < https://www.theguardian.com/technology/2019/jul/02/tiktok-under-investigation-over-child-data-use> accessed 16 February 2021.*

concerning the infringement of personal data from said application. With the 06.08.2020 executive order, the U.S. administration argued that TikTok and WeChat collect data from American users that could be retrieved by the Chinese government, while threatening to impose fines of up to $1 million and up to 20 years in prison for violation of the above order.[3]

Meanwhile, the situation in Europe is evolving in another direction with regard to this application. The Italian Independent Authority for the Protection of Personal Data has decided to temporarily block access to the TikTok web platform for users whose age has not been established with certainty, on the occasion of the death of a ten-year-old girl.[4] Moreover, Data Watchdogs in France, the Netherlands, Denmark and the U.K are investigating the social media app's compliance with the General Data Protection Regulation (GDPR).[5]

Furthermore, the latest challenge on TikTok, known as the "Silhouette Challenge" has sparked a wave of reactions from users, being accused of a flagrant violation of their personal data. This challenge started as a body positive movement and empowered women to celebrate their bodies in sensual sides. The challenge requires participants to film two separate videos of them and then combine them while using audio from TikTok. The videos start with the person standing in front of the camera in regular lighting while wearing casual clothes, with some choosing to wear nightwear, while in the following frame the camera filter turns red. The lighting perfectly shows off every curve as the participants strike different poses while standing in a doorway using an outside light source to create a shadow effect. Some chose to do it fully nude, while others wore underwear or bikinis. However, after the success of the challenge, applications were developed providing instructions on how one can remove the red filter and reveal the poses of TikTok's unsuspecting users, either naked or in their underwear. The red filter, that creates an atmosphere and supposedly hides the characteristics of the users' faces and other details, can easily be removed. After reactions and complaints about blackmail, one of the applications removing the filter was disabled.[6]

Given the direct mobilisation of governments, one can understand the importance of protecting privacy in modern society. Privacy constitutes a fundamental

---

3 *Ana Swanson, David McCabe and Jack Nicas, "Trump Administration to Ban Tik Tok and WeChat From U.S App Stores", (The New York Times, 18 September 2020), <https://www.nytimes.com/2020/09/18/business/trump-tik-tok-wechat-ban.html>, accessed 16 February 2021.*

4 *Agence France-Presse, " Italy blocks Tik Tok for certain users after death of a girl allegedly playing 'choking' game", (The Guardian, 23 January 2021), <https://www.theguardian.com/world/2021/jan/23/italy-blocks-tiktok-for-certain-users-after-death-of-girl-allegedly-playing-choking-game>, accessed 16 February 2021.*

5 *Saqib Shah, "TikTok privacy probes in Europe raise stakes for local data handling", (S&P Global, 1 October 2020), <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/tiktok-privacy-probes-in-europe-raise-stakes-for-local-data-handling-60562927>, accessed 16 February 2021.*

6 *Udi Tirosh, "Tik Tok Silhouette Challenge gone horribly wrong as the Internet finds a way to remove the red filter", (DIY Photography, 7 February 2021), <https://www.diyphotography.net/tiktok-silhouette-challenge-gone-horribly-wrong-as-the-internet-finds-a-way-to-remove-the-red-filter/>, accessed 16 February 2021.*

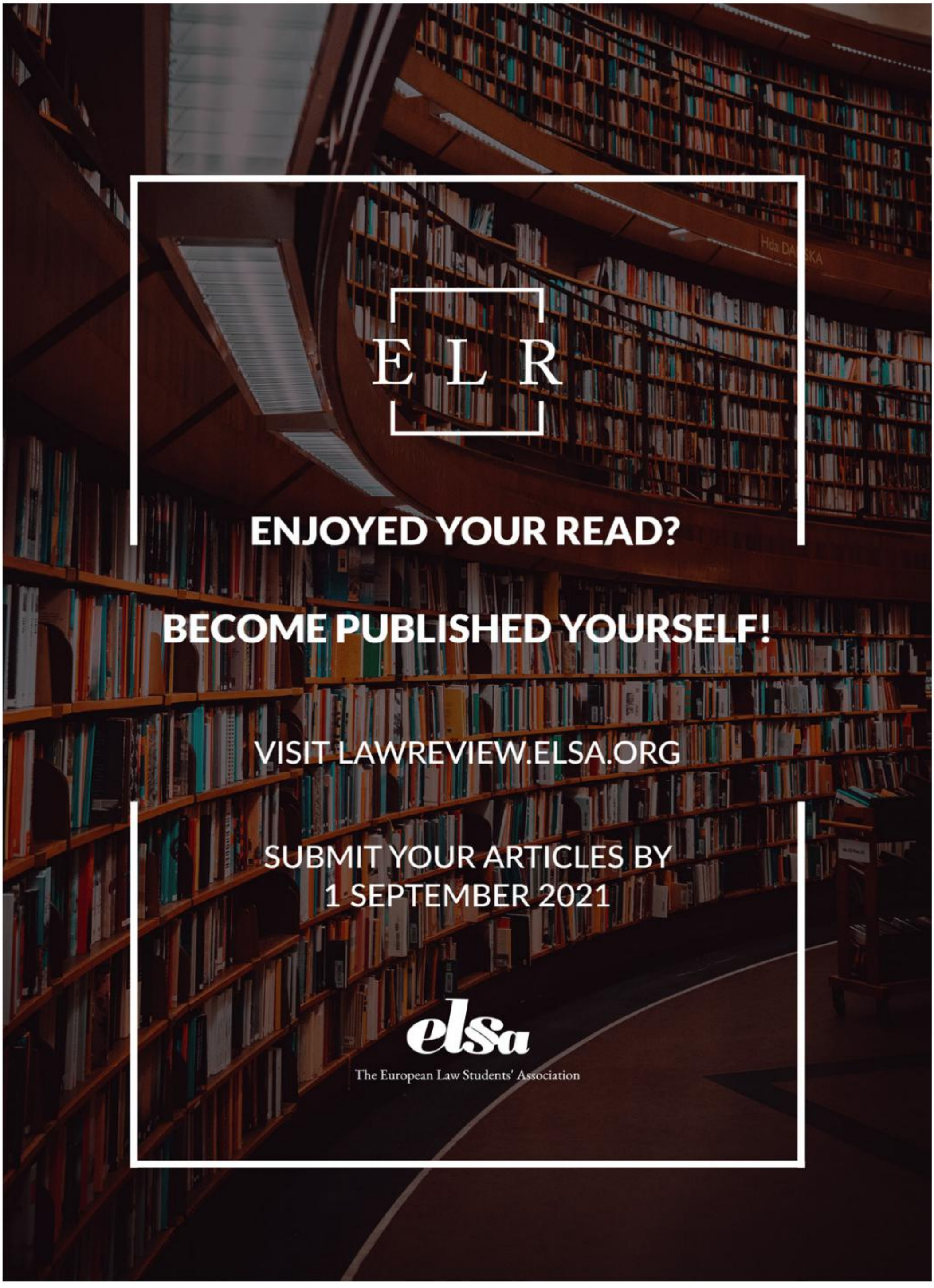
human right and its protection is frequently seen as a way of defining how far society can intrude into a person's affairs. No one should be subjected to arbitrary interference with their privacy, family, home or correspondence, or to attacks against their honour or reputation. Everyone is entitled to legal protection against such interferences or attacks.

On one hand, governmental interventions in favour of data privacy protection investigating popular applications and, in some countries, prohibiting their use, are not considered a minor task. The legislation's focus on individual data rights places individuals at the centre of privacy practices and the process of complying with its detailed requirements can force companies to monitor more closely the data they are collecting, their uses and the ways they store and share it. There is, therefore, a visible active effort to reduce data breaches.

On the other hand, despite the action of most governments and the adoption of new legislation, more and more information about each individual is being generated by more and more devices or applications, and it seems impossible to keep up.

Nevertheless, there should be a deeper reflection on the fact that there are individuals who are indifferent to the fact that they have offered the possibility of an excessive invasion to their privacy. Most applications used store an excessive volume of data on their user, while said data is often particularly sensitive. It is beyond doubt that there are a number of technical and legal issues rendering the protection of personal data in modern times particularly problematic. With the legal framework being extremely broad, the corresponding EU regulations and directives being enormous, there is an inability of staying up to date even by experts.

Taking the above into consideration, perhaps more important than any legislative initiative is the logic with which the users themselves comprehend the concept of privacy, and thus perceive the meaning of privacy. Each one produces more and more data, which are of considerable value and should therefore be managed wisely.


E L R
ENJOYED YOUR READ?
BECOME PUBLISHED YOURSELF!
VISIT LAWREVIEW.ELSA.ORG
SUBMIT YOUR ARTICLES BY
1 SEPTEMBER 2021
elsa
The European Law Students' Association

Is Europe capable to keep up with the digital revolution and its impact on children's privacy and data protection?

CHILDREN'S RIGHTS TO PRIVACY AND DATA PROTECTION IN A DIGITAL ERA

Raya Dimitrova
Member of ELSA Strasbourg

Article 16 of the Convention on the Rights of the Child provides that: 'No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.' The UNCRC was adopted in 1989; however, in the last thirty years, we witnessed a digital revolution – the use of social media and digital content is a major part of everyday life of every one of us, including children.[1] Interactive toys engage in conversation with children, record their voices and may also transfer the data to advertising and analytics companies. Some toys contain medical sensors which monitor children's body temperature and heart rate. Connected robots might include voice recognition and facial tracking.[2] Due to Covid, 1.2 billion children in 186 countries are affected by school closures[3] are turning to e-learning through various different digital platforms, collecting users' data. We witness how children rapidly transform from 'consumers' to 'data subjects.'

The question that arises is to what extent children throughout Europe can exercise their right to privacy in today's increasingly digital society.

Although international and national human rights

1 *Andreas Molander Skavlan, Social Media : What about children's privacy rights ?, (Gerrish Legal, November 2019), < https://www.gerrishlegal.com/legal-blog/2020/1/21/social-media-what-about-childrens-privacy-rights >, accessed 15 February 2021*

2 *Ingrida Milkaite and Eva Lievens, 'Towards a Better Protection of Children's Personal Data Collected by Connected Toys and Devices', (Digital Freedom Fund, 2018), < https://digitalfreedomfund.org/towards-a-better-protection-of-childrens-personal-data-collected-by-connected-toys-and-devices/>, accessed 5 February 2021*

3 *UNESCO, COVID-19 Impact on Education, 2020, < https://en.unesco.org/covid19/educationresponse>, accessed 7 February 2021*

instruments acknowledge that 'everyone' has a right to privacy, in practice, 'everyone' is presumed to be an adult. Even the fundamental principle of the best interest of the child is rarely considered while instruments of privacy protection are negotiated and adopted.[4] Is Europe capable of keeping up with the digital revolution and its impact on children's privacy and data protection?

Council of Europe

The rights to privacy and data protection are guaranteed by Article 8 of the European Convention on Human Rights[5] and the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). This Convention 108 has recently been modernised and now its Article 15 explicitly requires the authorities to pay 'specific attention [...] to the data protection rights of children and other vulnerable individuals'. The provisions of the ECHR and Convention 108 are applicable to all individuals, including children.[6]

In the recent years, the Committee of Ministers of Council of Europe adopted various recommendations and declarations – the 2008 Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, the 2014 Recommendation on a Guide to human rights for internet users and the 2016-2021 Strategy for the Rights of the Child, which acknowledged the importance of protecting the children's rights to privacy and data protection in digital environment.

Moreover, on 6th of February, the Council of Europe published 'Handbook for policy makers on the rights of the child in the digital environment' in order to support the implementation of Recommendation CM/Rec (2018)7 of the Committee of Ministers.[7] The Handbook examines different strategies to implement children's right to privacy and data protection, it states that: 'It is the primary obligation of the State to respect, protect and fulfil the right of the child to privacy and data protection'. The Handbook provides a checklist as to what a national data protection law should include : measures to ensure that children's personal

4 *Ingrida Milkaite and Eva Lievens, Children's Rights to Privacy and Data Protection Around the World : Challenges in the Digital Realm (2019) 10 (1) EJLT < https://ejlt.org/index.php/ejlt/article/view/674/912>, accessed 24 January 2021*

5 *Axel Springer AG v Germany App no 48311/10 (ECtHR, 10 July 2012), para 83; S and Marper v United Kingdom App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008), para 103.*

6 *K.U. v Finland, App no 2872/02, (ECtHR, 2 December 2008)*

7 *Available at < https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>, accessed 13 February 2021*

data is processed fairly, lawfully, accurately and securely; data minimisation principle; data protection impact assessment mechanisms; restrictions on the processing of special categories of data that are considered sensitive; requirements to provide easily accessible, meaningful, child-friendly and age-appropriate information on how data is collected, stored, used and disclosed; prohibition of profiling of children and establishment of an independent data protection authority. The Handbook also recommends awareness-raising strategies for children, parents and business enterprises to Member-States.

European Union

The European Union provides for the protection of both the right to privacy and the right to data protection through its primary and secondary legislation.[8] Article 7 of the 2000 Charter of Fundamental Rights of the European Union (CFREU) emphasises on the protection of privacy. Article 8 CFREU revolutionary recognises the particular right to data protection by providing that 'everyone has the right to the protection of personal data concerning him or her [and] such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law [...]'. Crucially, Article 24 CFREU explicitly acknowledges the rights of the child and states that 'children shall have the right to such protection and care as is necessary for their well-being'. Article 24 CFREU also emphasises that 'the child's best interests must be a primary consideration', making implicit reference to Article 3 UNCRC.

In addition, in April 2016, the Council and the Parliament of the European Union adopted a new instrument in the context of the EU data protection reform – the General Data Protection Regulation (GDPR). The GDPR includes a number of provisions that explicitly aim to protect the child's right to data protection. In particular, Article 38 recognises that 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.' Also, Article 8 emphasises on the conditions applicable to the child's consent – the general rule provides for a parental consent requirement for all youth under 16 years old in situations where information society services are offered directly to them, and consent is the lawful ground on the basis of which the data is processed. However, Member States may choose a lower age than 16, but not below 13.[9]

Furthermore, when it comes to automated individual decision-making (deciding solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual), Article 22 of GDPR is silent regarding children. Nevertheless, Recital 71 holds that automated decision-making and profiling 'should not concern a child'. This general prohibition is not in the GDPR provisions and is considered not as an absolute prohibition, but rather an expression of the high threshold when the data subject is a child.[10] Article 29 Working Party confirms that there is no absolute prohibition on the profiling of children in the GDPR, but data controllers should in general refrain from profiling children for marketing purposes.

Conclusion

In conclusion, in recent years, both the Council of Europe and the European Union established a legal regime which has the potential to serve as a foundation for the adoption of a more sophisticated regulatory framework, with stronger safeguards and enforcement mechanisms.

Meanwhile, data protection laws in Europe still leave considerable room for interpretation by Member States. Therefore, the National Data Protection Authorities and the European Data Protection Board (established by the GDPR) become key actors in the enforcement of the obligations. They, alongside with the national and supranational Courts, will play a major role in the next years to ensure the highest level of protection of children's privacy throughout Europe.

Above all, awareness-raising campaigns should be further promoted for children, parents and companies. It is crucial to understand that techniques such as profiling are dangerous, not only for the privacy of the child, but also for its right to receive information, freedom of thought and right to development - only by having access to different information, children grow to be critical-thinking, broad-minded, well-informed adults. By ensuring children's right of privacy in the digital era, we are also promoting children's rights and human rights as whole.

8 *Ingrida Milkaite and Eva Lievens, Children's Rights to Privacy and Data Protection Around the World : Challenges in the Digital Realm (n 3)*

9 *Ingrida Milkaite and Eva Lievens, 'Status quo regarding the child's article 8 GDPR age of consent for data processing across the EU' (Better Internet for Kids, 1 July 2019) <https://www.betterinternetforkids.eu/practice/awareness/article?id=3017751>, accessed 13 February 2021*

10 *Skavlan, (n 1)*

Protection of the right to privacy and how not to forget about the right to be forgotten

THE RISE OF SURVEILLANCE TECHNOLOGY: THE END OF PRIVACY AS WE KNOW IT?

Katja Kreft
Member of ELSA Ljubljana

In his dystopian science fiction novel, "1984", published in 1949, George Orwell wrote of a future where people are subjected to constant mass surveillance and propaganda. With the development of digital technology and the rise of corporations, capable of mass processing and storage of personal data, such as Google and Facebook, Orwell's idea of society is no longer science fiction, but a reality. While new technologies make an important contribution to the development of society, they impose many challenges some of which will be further discussed in this article.

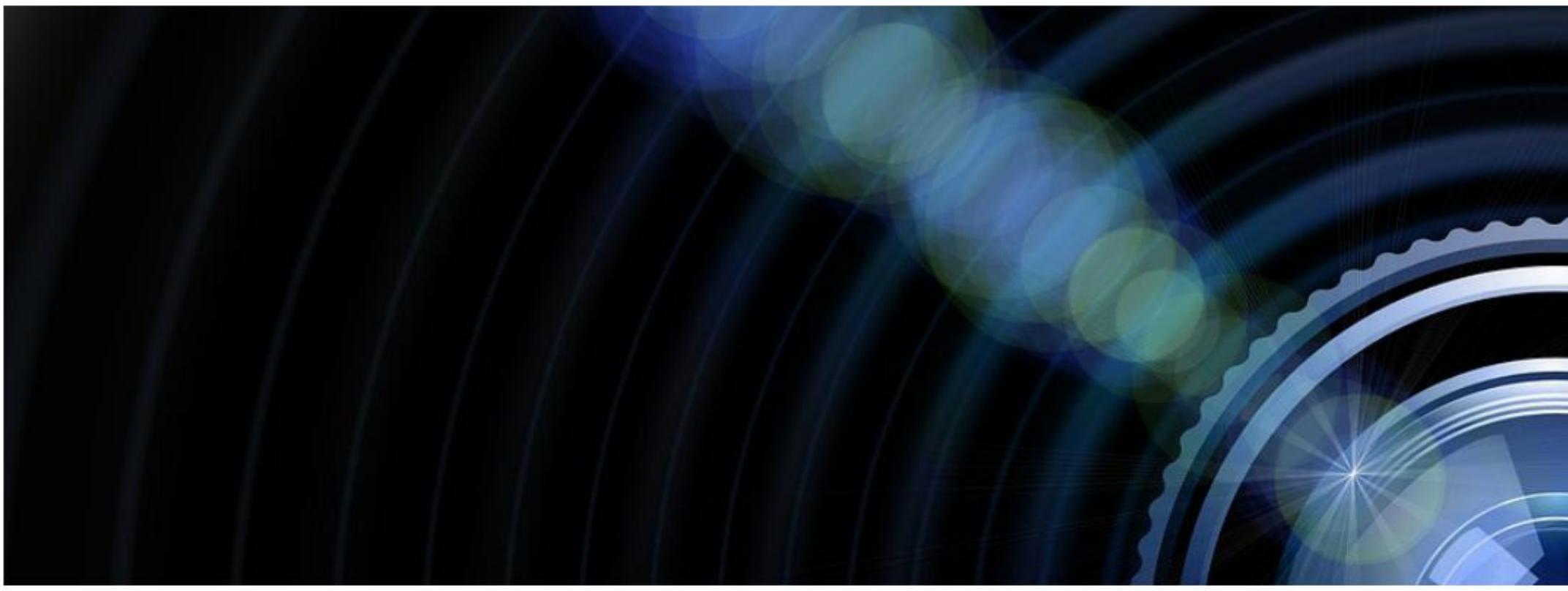
Protection of the right to privacy, and how not to forget about the right to be forgotten

The right to privacy entered into legal language in 1890, with the article "The right to privacy",[1] by Samuel Warren and Louis Brandeis, who argued that the legal system needed to recognise the right to privacy as, when information about an individual's private life is made available to others, it can injure the very core of an individual's personality. Despite the broad protection of the right to privacy[2], the advancement of technology inevitably causes new possibilities for unlawful interference. In today's digital era, it is impossible to keep track of or control all our personal data. This makes the very concept of privacy increasingly illusory, and raises questions that are likely to shape not only the future form of cyberspace but also the political, social, and economic interactions.[3] With that in mind, the European Union (EU) recognised that, to be able to secure the fundamental right for personal data protection, a unified and uniform approach is needed. A clear step in this direction was the reform of the data protection laws and the adoption of the

1 *Samuel D. Warren, Louis D. Brandeis, The Right to Privacy, (Harvard Law Review, Vol. 4, No. 5 1890) 193.*

2 *Art 8 of the European Convention on Human Rights, Art 12 of the Universal Declaration of Human Rights, Art 17 of International Covenant on Civil and Political Rights, Art 11 of the American Convention on Human Rights, Art 21 of the ASEAN Human Rights Declaration, Art 16 and 21 of the Arab Charter on Human Rights.*

3 *Shirin Elahi, Privacy and consent in the digital era, Information security technical report 14 (2009) 113–118.*



General Data Protection Regulation[4] (GDPR), which incorporated the right to be forgotten in Article 17. Since then, the right to be forgotten, or the right to erasure, has been gaining ground worldwide. The term "erasure," however, is misleading, as the content (personal data) does not actually get deleted on your request, but merely no longer appears in search results. Due to conflicts in its interpretation and practical issues regarding its implementation, the right to be forgotten is still largely debated. The Court of Justice of the European Union has dealt with Google's obligations regarding the right to be forgotten in three cases. In the first[5], a landmark ruling in 2014, the Court extended the interpretation of the right, and ruled that individuals have a right to delisting, meaning they can request that the search engines delist certain links from their search index if the results contain personal information that is 'inadequate, irrelevant, or no longer relevant, or excessive'. In the second case[6], the Court held that search engine operators must carry out a balancing act of the right to personal data protection with the freedom of expression and information, to prevent publishing content with sensitive personal data. In the last case[7], the Court assessed the territorial aspect of Google's obligations. It held that, under EU law, Google is not obliged to apply the right to be forgotten on all its servers around the world, only in the EU, which ultimately means that the right is curtailed for EU citizens as well. Proof that stronger and more precise protection of privacy is needed is represented in the 1.2 million requests for erasure that Google received last year. While it is impossible, in general, to remove personal data from the Internet once it was published, and limiting its accessibility might be the next best solution, the legal framework should place more focus on initial unlawful processing and storage of personal data.

Due to an increase of "opt-in" and "opt-out" mechanisms in the internet era, there is a growing tension between legitimate use of private data and privacy. A study by the Norwegian Consumer Council[8] found that health and fitness applications like MyFitnessPal and Runkeeper violate users' privacy by retaining their data, which they obtain on the basis of consent, for an indefinite amount of time, by tracking location even when the app is not in use, as well as by not disclosing which partners they share data with. Intrusive COVID-19 contact-tracing applications are of a similar nature. Also, in the context of the COVID-19 pandemic, governments around the world implemented the use of other invasive surveillance technologies, such as facial recognition or body temperature measurement. In South Korea, citizens who have breached mandatory quarantine have been forced to wear electronic bracelets which have the ability to alert the authorities whenever a person tries to remove them, or leave their confinement space.[9]

4 *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 (GDPR).*
5 *Case C-131/12 - Google Spain and Google, ECLI:EU:C:2014:317.*
6 *Case C-136/17 - GC and others, ECLI:EU:C:2019:773.*
7 *Case C-507/17 – Google, ECLI:EU:C:2019:772.*
8 *The Norwegian Consumer Council, Forbrukerradet < https://www.forbrukerradet.no/side/fitness-wristbands-violate-european-law/l> accessed 19 October 2020.*
9 *Lusa. Covid-19: Coreia do Sul vai usar pulseira eletrónica para quem violar quarentena Visão (2020) <https://visao.sapo.pt/atualidade/politica/2020-04-11-covid-19-coreia-do-sul-vai-usar pulseira-eletronica-para-quem-violar-quarentena/?fbclid=IwA R1rxucfzqmRI-9ta072qI5F3I4AYzyGQMCceeJo4dsPzbT_NU-CakCWqFik> accessed 14 February 2021.*

Those measures pose new threats to our privacy, freedom and democracy. What is especially concerning is the risk of the implemented extraordinary measures becoming permanent, and that mass surveillance and processing of personal data gets accepted as the new normal. Unfortunately, there are already a number of countries where the pandemic is being used to erode democracy and the right to privacy is being bridged under the pretence of protecting public health. In Russia, new rules have been applied against fake news about the virus, which reflected in increased persecution of independent media, something also seen under Viktor Orbán's regime in Hungary, and in Serbia and Turkey as well. While it is true that States have, according to the European Court of human rights case law[10] and international law[11], a number of positive obligations regarding the right to health, it is important that data protection principles are respected, even in particularly difficult situations[12] such as the current pandemic.

Conclusion

The modern technology at the disposal of States has enormous potential for surveillance which often threatens individual privacy. During the pandemic, governments around the world are undermining human rights compliance and there is a grave risk of totalitarian governments taking advantage of the installed surveillance technologies, even once the crisis is over. Additionally, stemming from Art 17/3 of GDPR, the data subject cannot count on their right to be forgotten when there is a public interest in public health. This right was described in the article as already insufficient due to its territorial application and ambiguity, and this exception contributes to the weaker protection of personal data. However, even in a pandemic situation, personal data protection should not be forgotten. Therefore, any personal data processed by States, private corporations and other data controllers must be in accordance with GDPR requirements and assessed on a case-by-case basis. As both, the right to privacy and the right to health are indispensable objectives of the general welfare, diligent balancing must be done between those interests to ensure that personal data protection is not neglected for the sake of public health. A positive step towards this goal is represented in an unprecedented partnership of Google and Apple, and their efforts to develop a contact tracking technology, based on Bluetooth, which allows the reduction of the virus spread while setting limits on the type of data that can be sent to the public authorities.[13] In the future, it is important that States invest more in technology that safeguards the right to privacy, since they can only build the trust of their citizens if complete transparency regarding the way surveillance technologies are designed and used is guaranteed.

10 *Vasileva v Bulgarie, app. no. 23796/10, §§63-69; Ibrahim Keskin v Turkey, app. no. 10491/12, §61; Jurica v Croatia, app. no. 30376/13, §84; Mehmet Ulusoy and Others v Turkey, app. no. 54969/09, §82.*

11 *Art 25 of Universal Declaration of Human Rights, Art 12 of International Covenant on Economic, Social and Cultural Rights.*

12 *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018.*

13 *Apple and Google partner on COVID-19 contact tracing technology (2020) <https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/> accessed 14 February 2021.*

REGULATORY CHALLENGES RELATING TO PRIVACY IN THE DIGITAL ERA

Maria Oikonomou Makrygianni
National Researcher in ILRG 2021 on Human Rights and Technology

INTRODUCTION

The Internet, and the opportunity for worldwide and anonymous communication it offers, have been widely considered hallmarks of free, democratic expression and deliberation. However, as it continues to grow and transform our lives, we should not ignore the real harms people face online. Among the human rights threatened by the development of new technologies, is the right to privacy recognised in Article 7 (respect for private life) and 8 (protection of personal data) of the Charter of Fundamental Rights?

PART I: CHALLENGES OF DEVISING SUITABLE REGULATION

There are many different practical challenges of devising regulatory mechanisms for privacy and data protection. Particular sources of regulatory challenges include the transnational nature of issues owing to the global nature of digital networks, which makes collecting, reproducing and disseminating personal data easier to do, more likely to be done in a way and on a scale that is harmful to data subjects, and more difficult to prevent. The relevant experience has also revealed the difficulty of finding a clear regulatory target. More precisely, the notion of privacy has turned out to be 'embarrassingly difficult to define'.[1] Privacy, fundamentally important though it may be, is an unusually slippery concept, despite intuitionist arguments supporting that human beings have a direct, common intuitive grasp of right and wrong in relation to privacy issues. For instance, the notion of privacy in Europe (an aspect of respect and personal dignity which often trumps freedom of expression) is radically different from the notion of privacy in the United States (an aspect of liberty against state intervention, often inferior to freedom of speech).[2]

Another key challenge in the field of privacy protection is the different regulatory objectives that firms and States want to achieve. According to Zuboff, ISPs, hiding behind the regulatory target of ensuring freedom of expression, argue for fewer legal regulatory duties aiming to obtain more data from their consumers in order to commercially exploit it. She argues that big data should not be considered a technology or an inevitable technological effect. On the contrary, they are the 'foundational component in a deeply intentional and highly consequential new logic of accumulation: surveillance capitalism',

1 *James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 The Yale Law Journal 1151, 1153.*
2 *Ibid, 1161.*

which aims (through extensive data extraction from e.g., computer-mediated action, such as Facebook 'likes' and Google searches, electronic transactions, databases etc. and analysis) to predict and modify human behaviour in order to produce revenue and market control. This type of constant surveillance appears not to erode privacy rights but rather to redistribute them, to concentrate them unevenly within the surveillance regime.[3] It is important to add that ISPs are also most likely to introduce privately enforced standards based on cost reduction and profit maximisation rather than legal obligations to ensure data protection, since the latter could create for some a disproportionate economic burden and affect the freedom to conduct a business (Article 16 CFR).[4]

Moreover, it must be noted that private intermediaries are implicitly, through technological and administrative designs, taking an increasingly central role in regulating civil liberties. This phenomenon has been characterised by De Nardis & Hack as the 'ongoing privatization of Internet governance'.[5] At first glance, private intermediaries appear to be content-neutral in that they provide intermediation of content provided by others rather than creating content and programming. Similarly, they seem to provide users with the opportunity to regulate how information is shared with their networks and the larger public. Beneath this visible layer, however, not only do they make day-to-day decisions about what content is allowed on their platform and the conditions under which this content should be removed, playing a decisive role in promoting or constraining free speech (Article 11 CFR), but also collect and aggregate a wide range of both content and accompanying user data and metadata. At the same time, private intermediaries generally share a great deal of this information with external entities: with third parties in order to maximize online advertising revenue generation and after external requests from governments to disclose user data for rationales as diverse as law enforcement, national security, defamation or political oppression.[6] This delegation of public attributions to Internet intermediaries could be considered hazardous, taking into account that they,

3 *S Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75, 75, 78-80, 83.*

4 *Luca Belli & Christina Sappa, 'The Intermediary Conundrum: Cyber-Regulators, Cyber-Police or Both?' (2017) 8 (3) JIPITEC 183, 196.*

5 *Laura DeNardis & Andrea M. Hackl, 'Internet governance by social media platforms' (2015) 39 Telecommunications Policy 761, 763.*

6 *Laura DeNardis & Andrea M. Hackl (n 5), 765.*

in contrast with formal administrative bodies, do not have a positive obligation to protect human rights and to operate transparently, impartially and in the public interest.[7]

PART II: EU RESPONSE

The general response, at an EU level, in relation to the regulation of data has been to adopt supranational regulations with the introduction of new rights (e.g., data protection rights) and new enforcement tools with the right to be forgotten originally developed in Google v Spain[8] and ultimately codified in Article 17 GDPR as well as to introduce property mechanisms for non-personal data as discussed by the EU Commissioner Breton.[9] In other words, EU regulatory efforts have largely focused on protecting personal data, first, through the e-Privacy Directive regulating their electronic communication between parties, the recognition in the Lisbon Treaty of privacy and personal data as fundamental rights and, more recently, through the General Data Protection Regulation regulating the unlawful processing of data in order to ensure its protection. Instead, with regards to non-personal data, the EU has sought to encourage its generation and exploitation, as so-called 'non-personal' or industrial data are a growing focus of regulatory initiatives, characterised as a key new type of economic asset and the 'lifeblood of the global economy'.[10]

Apart from Google vs Spain, where, as aforementioned, the right to be forgotten online was recognised, the CJEU in several other rulings has contributed in the recognition, development and strengthening of the right to privacy. In Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources[11], the CJEU held that a European Union directive requiring ISPs to store telecommunications data in order to facilitate the prevention and prosecution of serious crime was invalid under Articles 7 and 8 CFR. Similarly, in the joined cases Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home

7 *Belli & Sappa (n 4), 186.*
8 *C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ECLI:EU:C:2014:317 [88] [99].*
9 *Javier Espinoza & Sam Fleming, 'Europe urged to use industrial data trove to steal march on rivals' Financial Times (Brussels, 14 January 2020) < https://www.ft.com/content/8187a268-3494-11ea-a6d3-9a26f8c3cba4> accessed 21 February 2021.*
10 *European Commission, 'Enter the Data Economy: EU Policies for a thriving data ecosystem' EPSC Strategic Note Issue 21 (11 January 2017), 1.*
11 *C–293/12 Digital Rights Ireland Ltd ECLI:EU:C:2014:238 [29] [37-39] [65-69].*

Department v. Watson[12], the CJEU, in a preliminary ruling, found that national legislation establishing mass surveillance of electronic communications for the purpose of fighting crime violated the right to privacy and the right to data protection and that national legislation allowing for general and indiscriminate data retention for the purpose of fighting crime must specifically comply with these rights.

In Google v CNIL[13], the Court of Justice held that there is no obligation under EU law for Google to apply the European right to be forgotten globally. While Google and proponents of the freedom of expression have claimed this case as an ostensible win, a closer analysis may lead to a different conclusion. To begin with, in its landmark ruling, the CJEU emphasised the goal to provide a high level of protection of personal data throughout the EU. Accordingly, it held that search engine operators are required to remove all the links on all the versions in the EU regardless of where the request to de-reference originates in the EU. Furthermore, paragraph 72 of the judgment reveals the effort to establish the lawfulness of global de-referencing as a general principle: by finding that EU law does not prohibit it and that Member States remain competent to order search engine operators to de-reference globally after balancing the conflicting rights of personal data protection against the right to freedom of information under national standards of protection of fundamental rights, the Court left the door wide open for the possibility of global de-referencing as determined by a national DPA or a national court in the EU.

CONCLUSION

To conclude, it can be observed that the right to privacy is interconnected with other human rights, such as the freedom of expression, and is significantly affected in the digital era. Taking into account the various challenges in devising a suitable regulatory framework and the EU efforts, at a legislative and judicial level, to protect personal data, it could be supported that privacy challenges would be better addressed through concerted and multi-stakeholder engagements involving not only states and companies but also civil society, academics and scientific/technical communities.[14]

12 C–203/15 and C–698/15 Tele2 v Postoch telestyrelsen ECLI:EU:C:2016:970 [93-94] [100-101] [108].
13 C-507/17 Google v CNIL EU:C:2019:772 [52-51] [54] [66] [72-73].

14 United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age" (2014), 16.

PRIVACY RIGHTS IN THE DIGITALISED ERA - AN OVERBEATEN PIPE DREAM ALL OF US SHOULD CARE ABOUT? A SHORT EXPLORATION

Lena Anna Kuklińska
Vice President in charge of Marketing at ELSA the Netherlands, Assistant for Marketing Development at ELSA International

It has been said that no other right has received as much attention in the digital era as the right to privacy.[1] Privacy as a human right is enshrined in the United Nations Declaration of Human Rights (UDHR) 1948, Article 12: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'; and many other international conventions. Privacy allows us to create personal barriers and decide who can infiltrate them.[2]

Innovation brings solutions, yet, more often than not, it does so while simultaneously creating new challenges for various areas of societal functioning. Unwilling or incapable of adjusting at an adequate pace, law is struggling to embrace Uber, drones, Facebook and many other developments that we do not know yet but will be infatuated with tomorrow. Information technology, the convergence of data processing with communication,[3] has been one of the bigger 'opponents' law has had to face.[4]

We are seeking ways of tightening the regulation just so the privacy of individuals is protected with each new technology entering the scene; yet, the question that should be asked is: is it even worth trying? Will we ever be able to invest a sufficiently protective law which would work no matter what comes after TikTok or Google? Is the regulation of privacy in the digitalised world even feasible? And despite what the answer is, should we persevere through?

To be able to answer these questions, we ought to look at what has already been achieved, and the consequences of it. The first example of a privacy law advancement that comes to mind is the General Data Protection Regulation of the European Union, whose aim is to improve privacy protection across all fields, placing the consent and one's mind at the heart of the regulation, in line with what the right to privacy

1 *Molly K Land and Jay D Aronson, New Technologies for Human Rights Law and Practice (Cambridge University Press 2018) 150.*
2 *'What is Privacy?' (Privacy International, 23 October 2017) < https://privacyinternational.org/explainer/56/what-privacy> accessed 25 January 2021.*
3 *Dennis Longley and Martin Shain, Dictionary of Information Technology (Springer 1982) 165.*
4 *Ramesh Chandra, Information Technology in 21st Century (Gyan Publishing House 2003) 136-137; Ian Lloyd, Information Technology Law (OUP 2020) 216.*

is under international law.[5] Despite the immense influence acknowledged in the reports of agencies and firms such as Deloitte[6], Varonisor[7] the EU itself[8], the regulation has been reported to have created, at worst, or overseen, at best, the ways of circumventing the laws included within, which contributes to identity theft, cybersecurity risks, silencing the freedom of expression and violations of the right to privacy and related human rights.[9]

Other examples of imperfect laws may be derived from the criticism directed at the Australian Commonwealth Privacy Act 1988, Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) 2000, or even from the inability of smaller units, such as the US states, to enforce appropriate regulations for years, if at all.[10] Frequently, the published laws fail because of their inability to comprehensively cover all the present and future breaches. The actors to question are the legislators and judiciaries, for their incapability to draft a law that would be interpreted to combat any new trick, and the innovators, who either create hazardous inventions or develop technologies which are circumventable. A prime example of the latter, to postpone the extensive exploration that the issues of malicious intent are owed, is data leaks, which, mostly associated with big platforms like Facebook, also happen within smaller units, of which the author of this article learnt from her own experience. Pixlr is an online photo editor which does not store any personal data except for email information and names of the person logging in. Nevertheless, as the email below proves, the database was hacked to source those details and, presumably, to send them to advertising companies.

If this was a one-time occurence for one person, it could probably be fairly unalarming, taken as a singular slip of an unprepared company, reprehensible yet bearable. Nonetheless, a while ago, the author also received a blackmailing SPAM email which mentioned one of the typical passwords that she uses, 'found', allegedly, being used on an adult content website (which is impossible to have occurred). The information must have been stolen or willingly given away by a platform registered at with that password. Learning which service it had been is most likely impossible. For years, we have been sharing so much information that finding who knows what about us, legally or not, is like

5 *Presidency of the Council, 2012/0011 (COD) (Council of the European Union, 11 June 2015) < https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> accessed 26 January 2021.*

6 *'Deloitte General Data Protection Regulation benchmarking survey' (Deloitte, 2017) < https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-readiness.html> accessed 26 January 2021.*

7 *Rob Sobers, ' A Year in the Life of the GDPR: Must-Know Stats and Takeaways' (Veronis, 17 June 2020) < https://www.varonis.com/blog/gdpr-effect-review/> accessed 26 January 2021.*

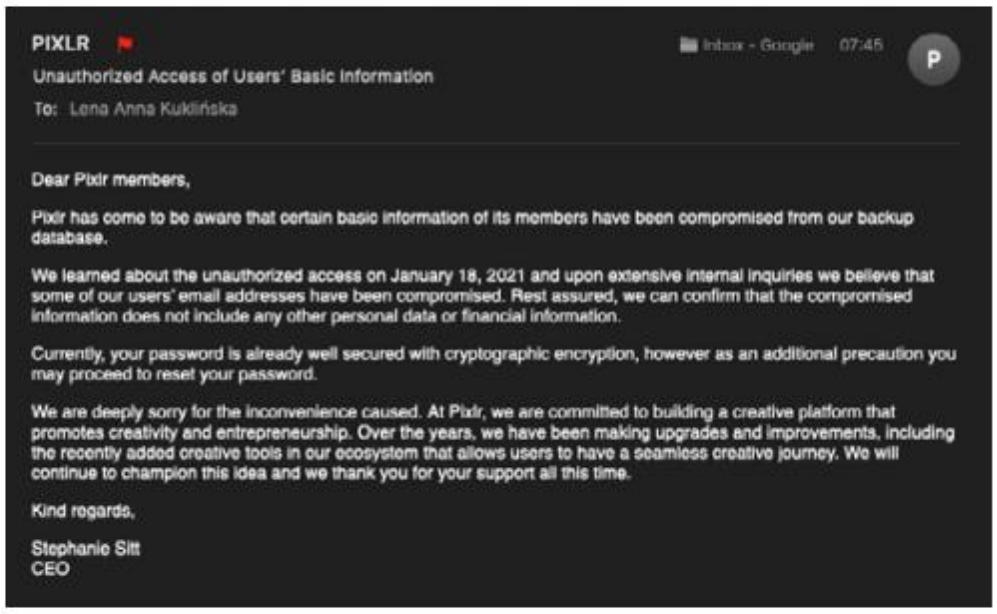
8 *'General Data Protection Regulation shows results, but work needs to continue' (European Commission, 24 July 2019) < https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449> accessed 26 January 2021.*

9 *Roslyn Lyton, 'The 10 Problems of the GDPR: The US can learn from the EU's mistakes and leapfrog its policy' (American Enterprise Institute, 12 March 2019) <https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf> accessed 26 January 2021; Md Rakibul Hoque and Edward R Bashaw, Cross-Border E-Commerce Marketing and Management (IGI Global 2020) 109.*

10 *As it is to be seen for Washington in the upcoming days; 'The Washington Privacy Act Gets its Third Bite at the Apple' (Vorys, 20 January 2021) < https://www.vorys.com/publications-2853.html> accessed 26 January 2021.*

	Not aware of the GDPR	Aware of the GDPR, but know nothing about	Know a bit about the GDPR	Know a lot about the GDPR
Comfortable sharing data	28%	28%	25%	39%
Clearer when info is collected	34%	38%	43%	53%
Better understanding of data rights	34%	39%	48%	59%
Comfortable with online behavioral advertising	34%	35%	35%	46%

GDPR has achieved a very difficult task – increased the awareness about data collection and protection among its subjects. Source: Statista (2021)..


PIXLR

Inbox - Google 07:45

Unauthorized Access of Users' Basic Information

To: Lena Anna Kuklińska

Dear Pixlr members,

Pixlr has come to be aware that certain basic information of its members have been compromised from our backup database.

We learned about the unauthorized access on January 18, 2021 and upon extensive internal inquiries we believe that some of our users' email addresses have been compromised. Rest assured, we can confirm that the compromised information does not include any other personal data or financial information.

Currently, your password is already well secured with cryptographic encryption, however as an additional precaution you may proceed to reset your password.

We are deeply sorry for the inconvenience caused. At Pixlr, we are committed to building a creative platform that promotes creativity and entrepreneurship. Over the years, we have been making upgrades and improvements, including the recently added creative tools in our ecosystem that allows users to have a seamless creative journey. We will continue to champion this idea and we thank you for your support all this time.

Kind regards,

Stephanie Sitt
CEO

Email received by the author of the article on the 26th of January 2021.

looking for a needle in the haystack. Notwithstanding, this further suggests that protection of privacy, either through law or technology, is unviable in the digital era.

As much as the conclusion of this short examination is bleak, it should not be discouraging but rather inspiring for those who believe that law can be drafted to protect its subjects duly. Asking whether we should be trying to invent newer, flawless laws could be answered manifoldly, depending on one's outlook on the world. Nevertheless, it should be considered that giving up on human rights frequently brings detrimental consequences, not only to the individual, since a stolen email could lead to the theft of more personal data or information, such as bank account credentials, but also to the society as a whole. Breaches of privacy rights have been deemed potent of creating a foundation for more penetrating and far-reaching human rights violations. The neglect of privacy leads to the infiltration into the lives of individuals, by governments or other actors, the limitation of the freedom of speech or the right to participate in the political life of one's country and the manipulation of the masses.[11] This becomes more familiar once the examples of the Chinese or Venezuelan legislative efforts are recalled. Taking their practices, it is seen that invasion of privacy is the first step, in the modern era, to solidify the governmental grip over a nation and to commence violations of rights of certain groups, be it religious, ethnical, sexual, or simply those opposing the powers that be. In China, over one million of Turic Muslims are being oppressed in detention centres and re-education facilities, under the procedure sprouted from individual surveillance and data-collection.[12]

Hence, it emerges that breaking one law often leads, to or facilitates, breaking another. If we neglect the protection of our personal information, we could lose not only our property but also our identities or freedom - the things that should matter even more than before given the present necessity of online interaction. Seeing what has been outlined above, it might be that we will never be able to protect our privacy as effectively as needed in the digital world, which thrives on innovation and finding new, creative ways of adaptation. Nevertheless, which should be the overall envoy of this article, we must try, just so we do not sell our freedom by recklessly pressing 'agree' on yet another cookie pop-up.

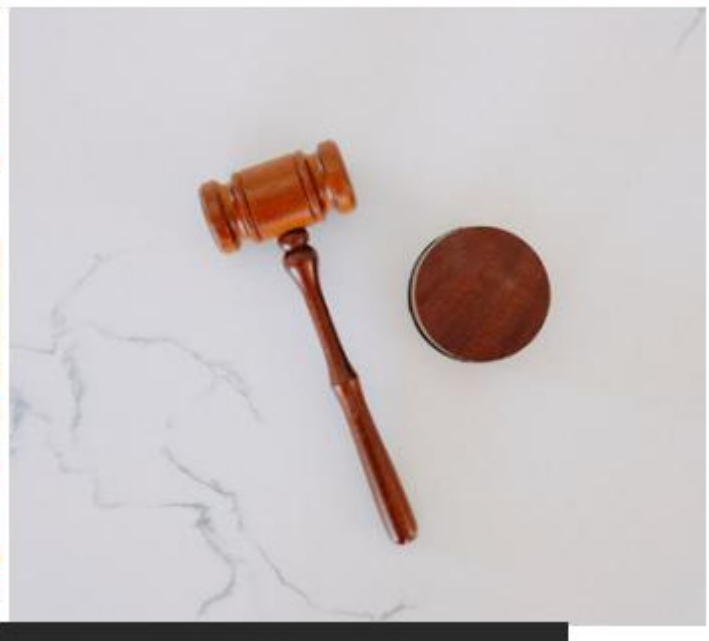
---

11 Molly K Land and Jay D Aronson, New Technologies for Human Rights Law and Practice (Cambridge University Press 2018) 157 – 158; 'Human Rights and Protection of Privacy: Even good laws do not prevent abuse' (Freedom Barometer, 13 February 2020) http://www.freedombarometer.org/blog/human-rights-and-protection-of-privacy-even-good-laws-do-not-prevent-abuse-90/ accessed 26 January 2021; Anita Allen, Unpopular Privacy: What Must We Hide? (OUP 2011) [pages unnumbered].

12 Deborah Brown and Anriette Esterhuysen, 'Why cybersecurity is a human rights issue, and it is time to start treating it like one' (APC, 28 November 2019) https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one accessed 28 January 2021; Kenneth Roth, 'China's Global Threat to Human Rights' (Human Rights Watch, 2019) https://www.hrw.org/world-report/2020/country-chapters/global# accessed 28 January 2021; Stakeholder Report Universal Periodic Review 26th Session - Venezuela (Bolivarian Republic of) 'The Right to Privacy in Venezuela (Bolivarian Republic of)' (Harvard Law, 2016) https://hrp.law.harvard.edu/wp-content/uploads/2016/04/venezuela_upr2016.pdf accessed 28 January 2021.

G.C. ECONOMOU & ASSOCIATES

LEADERSHIP
CREATIVITY
RESULTS



WHY US?

G. C. ECONOMOU AND ASSOCIATES LAW FIRM PROVIDES A COMPREHENSIVE SPECIALIST RANGE OF LEGAL, FINANCIAL, FIDUCIARY, PARA-LEGAL AND SECRETARIAL SERVICES TO LOCAL AND INTERNATIONAL SELECTED CLIENTS.

GCE ECONOMOU ASSOCIATES
WWW.GCE-ASSOCIATES.GR

Athens, Greece
11 Kanari Street, 10671
+30 2103640030
economou@gce-associates.gr

The European Law Students' Association