Palacký University in Olomouc

Faculty of Law

Bc. Adéla Krönerová

Digital Fundamental Rights in the case law of the Court of Justice of the European Union

Master's thesis

Olomouc 2022

"I hereby declar that this Master's thesis on the topic of Digital Fundamental Rights in the case law of the Court of Justice of the European Union is my original work and I have acknowledged all the sources used."

In Olomouc, 27 March 2022 ……..……...……

Bc. Adéla Krönerová

I would like to thank the supervisor of my Master's thesis, JUDr. Ondrej Hamulak, Ph.D., for professional guidance and for providing valuable advice and comments during the creation of this work.

Special thanks to Mr Graeme Dibble who read every single line to check the grammatical side of this work and contributed to its finalizing.

Table of Contents

List of Abbreviations

EU	European Union
ECHR	The European Convention on Human Rights
ECtHR	The European Court of Human Rights
CFR	The Charter of Fundamental Rights of the European Union
CJEU	The Court of Justice of the European Union
DSA	Digital Services Act
GDPR	General Data Protection Regulation
Ibid.	Ibidem (in the same place)
i.e.	Id est (that is)
RTBF	Right to be forgotten
TFEU	Treaty on the functioning of the EU

Introduction

In any democratic state governed by the rule of law, one of the most important and essential things is the protection of human rights and freedoms. This protection has evolved over the centuries and is constantly evolving; for example, due to the development of society or political systems. In my opinion, much has been achieved in this area in most of these states, and human rights are very well protected. One of the most developed areas that also affects human rights is technology. Although digitization can offer solutions to many of the challenges facing Europe and the world, digital technologies are also changing not only the way people communicate but more generally the way they live and work. The protection of EU values and the fundamental rights and security of citizens should be a key element of digitization. That is why in today's world it is inevitable to emphasize, address and ensure the protection of human rights and personal data in the digital sphere.

Digital rights are those rights that allow individuals to use, access and publish digital and electronic media and devices and to use computers and various technologies. The concept of digital rights mainly reflects the protection and implementation of existing rights in the digital world. I will use the term digital fundamental rights because the word fundamental expresses the group of rights that have been recognized with a high degree of protection. However, the protection of digital fundamental rights is not firmly enshrined in any binding EU document. It is still evolving and is based mainly on disputes that have already arisen and their judgments in the case law of the Court of Justice of the European Union. The CJEU case law responds to the ever-evolving digitization and seeks to ensure the protection of the rights of individuals. In the last few years this topic has become very important on the European continent and the rest of the world.

The reason for choosing the above topic is to outline and approach the issue of Digital Fundamental Rights in the EU, as the processing of personal data is an increasingly common problem. The provision of personal data on the internet has become a daily routine for almost all citizens and only a few of them realize the extent to which such information can be used against them. It can cast a shadow over our futures and the consequences can be serious. My aim will be to outline the issue of digital fundamental rights and freedoms of individuals in the EU and to analyse the rulings of the CJEU in this area, i.e. case law focusing on the right to be forgotten, data protection, privacy on internet networks and content regulation. In this thesis I will try to expand our knowledge and understand the implications of the judgments of this Court.

The main question this work addresses is: what are the implications of individual case law on the protection of the rights of individuals and the functioning of internet search engines? In this work, I set hypotheses that will either be confirmed or refuted based on the answers to the questions. This will be done using the appropriate research methods of descriptive method and analysis. The first hypothesis is: *'The CJEU case law responds effectively to the pace of development in the digital world, thus ensuring the reliable protection of individuals' digital rights.'* To confirm this hypothesis, a research question is set: How effectively can CJEU respond to technological developments and thus protect digital fundamental rights? The second hypothesis is: *'The RTBF is an adequate legal instrument for personal data protection.'* The question is: What kind of tool is the RTBF for the protection of digital fundamental rights? This Master's thesis will also show us which fundamental rights come into conflict in this area, and an analysis of the case law should therefore show how we defend ourselves in the digital world and ensure our privacy.

At the beginning of the work, a descriptive method will prevail, as I will try to outline the establishment of digital rights in the EU. The first chapter will focus on the protection of digital fundamental rights. It is necessary to focus on the Charter of Fundamental Rights of the EU, which enshrines fundamental rights, especially on the GDPR regulation, which is considered one of the most important legislative acts in the field of personal data protection. It will be important to define at the outset the RTBF, which has just been enshrined in the GDPR and which will be further discussed in the next part of the thesis. In the following chapters a method of analysis will be applied whereby I analyse the individual case law of the CJEU, which will be divided according to which rights and areas were chosen. As I spent the winter semester in Austria studying a double-degree programme, I consider it appropriate to devote a part of this Master's thesis to this state. Consequently, one of the topics will also involve cases relating to Austrian citizens. I will outline the Austrian legislation related to the GDPR and focus on the implications of the decisions of selected cases, which also greatly affect the protection of digital rights.

1 Protection of Digital Fundamental Rights in the EU

In the 21st century human rights include digital rights, which in today's developed technological world provide individuals with protection of data shared in the digital world and enable access to and publication of data on the internet. The internet is a global public good and therefore every state or international organization must create a legal environment that ensures its use, access and respect for universal human rights. In the internet world, therefore, rights such as freedom of expression, privacy and the right to information have been identified. Any limitations to the right of freedom of expression online must be provided for by law or a legitimate aim.[1] However, the problem arises when these rights are violated or applied in such a way that they interfere and conflict with the rights of others. EU law recognizes two forms of privacy protection. The first of these refers to the protection of personal data contained in the rules in the GDPR.[2] It operates according to instrumental logic and aims to give individuals control over their personal data. The second - dignified privacy, enshrined in Article 7 of the CFR - follows this logic and is intended to prevent personal injury caused by breaches to the rules of decency.[3]

Within the EU the protection of personal data is a fundamental right enshrined in Article 8 of the CFR and in Article 16 of the TFEU. As a powerful force, the EU can set certain standards for the protection of digital rights, which can serve as a basis for other states or organizations across world. Inspiration for the rest of the world came with the introduction of the GDPR which revised and harmonized outdated data protection rules that had been in place since 1995. It established a regime based on data protection as a fundamental human right and set the global standard for modern privacy protection.[4] However, the most important EU source in this area is the case law of the CJEU. Case law formulates European standards for the protection of human rights, in particular the judgment of the CJEU in Case Google Spain.[5]

---

[1] The INTERNET is a public good. *waccglobal.org* [online]. 27 August 2017 [viewed 15 January 2021]. Available from: https://waccglobal.org/the-internet-is-a-public-good/#:~:text=ARTICLE%2019%20believes%20that%20the,be%20both%20necessary%20and%20proportionate

[2] 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)

[3] POST, R. Data privacy and dignitary privacy: Google Spain, the Right to be forgotten, and the construction of the public sphere. Duke Law Journal [online]. 2018 [viewed 15 January 2021], p. 982. Available from: https://core.ac.uk/download/pdf/213019831.pdf

[4] BLANKERTZ, A and J. JAURSCH. How the EU plans to rewrite the rules for the internet. *brookings.edu* [online]. 21 October 2020 [viewed 15 January 2021]. Available from: https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-the-internet

[5] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, Judgment of the Court (Grand Chamber), 13 May 2014.

A new 'Right to be forgotten' has emerged, which is the right to be erased from the online environment and is now listed in the GDPR as a progressive new digital right.

The EU is now preparing The Digital Services Act which should have an even greater impact than the GDPR on creating a comprehensive framework for the functioning of digital services in Europe. This is a legislative proposal from the Commission which was submitted to the European Parliament and the European Council in December 2020 under the leadership of Ursula von der Leyen. If this proposal is approved, the legal framework of the EU will be updated. A major change should be the modernization of the e-commerce directive as well as new legislation on illegal content, transparent advertising and misinformation. EU law in its current form gives private companies a secure position in terms of responsibility for illegal content posted by users. However, the adoption of the proposal by the DSA would change this approach. This could lead to a situation where companies use censorship more and remove both legal and illegal content.[6] In January 2022, the European Parliament approved its position for negotiations with Member States and the European Commission by 530 votes by MEP's. Christel Schaldemose, who is the EU's lead legislator on the bill, said that the DSA could become the new gold standard for digital regulation in Europe and around the world.[7] The next step is negotiations with the European Council and the Commission. France, led by President Macron, wants to conclude the file before the end of its rotating presidency, but it is likely that this will happen during the Czech presidency. At the end of all the talks, the MEP's will vote on the final agreement.[8]

1.1 Charter of Fundamental Rights of the EU

As mentioned above, the basic document, the CFR, which governs the protection of human rights in the EU, includes rights that are also applied to the internet and which are adapting to the digital age because it is essential to convert the legislation on these rights to the new modern technological age.

[6] MCGOWAN, I. The Digital Services Act could make or break European democracy. *euractiv.com* [online]. 25 November 2020 [viewed 7 February 2021]. Available from: https://www.euractiv.com/section/digital/opinion/the-digital-services-act-could-make-or-break-european-democracy/

[7] European Parliament adopts draft of Digital Services Act. *openaccessgovernment.org* [online]. 21 January 2022 [viewed 27 January 2022]. Available from: https://www.openaccessgovernment.org/digital-services-act-2/128056/

[8] ZSIROS, S. What is the EU Digital Services Act and how will it impact Big Tech? *Euronews.com* [online]. 20 January 2022 [viewed 27 January 2022]. Available from: https://www.euronews.com/2022/01/20/what-is-the-eu-digital-services-act-and-how-will-it-impact-big-tech

Article 7 of the CFR establishes the right to respect for private and family life. 'Everyone has the right to respect for his or her private and family life, home and communications.'[9] Thus, the right to respect for privacy is guaranteed but this becomes contradictory on the internet, where people share a lot of private things which appear publicly on social networks and are visible to everyone. The next important right is set out in Article 8 which confirms the right to the protection of personal data, the observance of which is supervised by an independent authority. This personal data may be used only for specified purposes and on the basis of consent or in other circumstances stipulated by law.[10] Thus, in Article 7, the CFR refers to the right to privacy of individuals, but Article 8 refers specifically to the protection of personal data. It follows that the concept of personal data protection has been differentiated in terms of ensuring the protection and enforcement of the law relating to them, so that it does not have to rely on the interpretation of the CFR and the derivation of personal data protection from the right to privacy by the CJEU. [11] Such a procedure was used by the ECtHR, which concluded that Article 8 of the ECHR also applies to personal data.[12]

We can already see that the protection of personal data on the internet has to be well regulated because data sharing itself is an everyday activity for almost everyone. If personal data is published on the internet, this data is available indefinitely to an indefinite number of people. Therefore, any individual in the EU whose personal data is processed in any way and an infringement occurs may rely on this article as well as Article 16 of the TFEU. It is therefore important to strike a balance between legislation for the protection of personal data and the sharing of data on the internet.

Another fundamental right that must be mentioned in connection with the functioning of the internet is: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.'[13] This is set out in Article 11 as the freedom of expression and information right. Everyone has the right to express their opinions and find out information, including on internet networks. However, in today's digital world, restrictions on freedom of expression are necessary and enforceable by the courts. For example, this could involve slander or incitement to violence.

[9] Charter of Fundamental Rights of the European Union (2012/C 326/02), 2000, Nice, Article 7.
[10] Ibid., Article 8.
[11] *Amann v. Switzerland*, ECtHR, Application No. 27798/95, Judgement, 16 February 2000, Article 65.
[12] *Leander v. Sweden*, ECtHR Application No. 9248/81, Judgement, 26 March 1987, Article 48.
[13] Charter of Fundamental Rights of the European Union,…Article 11.

Unfortunately, the internet has changed its view on the right to privacy. In most cases, the right to privacy supports the right to freedom of expression. However, there are cases mostly on the internet where respect for privacy is contrary to the right to freedom of expression. The guaranteed right to privacy often conflicts with freedom of expression, as both rights do not provide for the automatic derogation from the other. Almost every step we take on the internet is an act of expression. We consciously support freedom of expression in a modern context and ignore our right to privacy which previously allowed and supported freedom of expression. In these conflicts the CJEU has the greatest say as it decides on these cases according to the circumstances.[14] In general, the courts favour an approach that puts the privacy of the individual above freedom of expression. On the other hand, it is more likely to side with the public interest and freedom of expression in cases involving public persons.[15]Article 52(1) of the CFR lays down rules if certain fundamental rights need to be restricted.

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[16]

At the same time, this article acknowledges the possibility of restricting fundamental human rights where necessary to protect the rights and freedoms of others. One of the best-known cases that the CJEU has had to deal with in terms of assessing infringements of Articles 7 and 8 of the CFR is the Digital Rights Ireland case of 2014.[17]

1.2 General Data Protection Regulation

The General Data Protection Regulation is the EU's general regulation on the protection of personal data, which significantly increases and ensures the protection of citizens' personal data. This new legal framework had proved to be very demanding in its scope, affecting a wide range of functioning information systems, processes and documents. GDPR was issued through the ordinary legislative process and was published in the Official Journal of the EU on 27 April

[14] MENDEL, T. and others. *Global survey on internet privacy and freedom of expression*. Paris: the United Nations Educational, Scientific and Cultural Organization, 2012, p. 95.
[15] GUADAMUZ, A. Developing a Right to be Forgotten. *University of Sussex* [online]. 2017 [viewed 4 February 2021]. Available from: https://www.researchgate.net/publication/320985071_Developing_a_Right_to_be_Forgotten
[16] Charter of Fundamental Rights of the European Union…, Article 52 (1).
[17] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12, CJEU, Judgment of the Court (Grand Chamber), 8 April 2014.

2016.[18] Thanks to GDPR, on the one hand, individuals have more control over their personal data, while on the other, it defines the obligations of those who process the personal data. The GDPR attempts to get institutions to think about the information they gather and about the way they organise and control personal data. The GDPR also helps to clarify the distinction between the right to personal data protection and the right to privacy.[19] Privacy and personal data protection are concepts that are interrelated and are often used interchangeably but they are two different concepts. According to the GDPR, we can associate privacy primarily with dignity and the rule of law and with the protection of 'personal space'. Data protection, in turn, concerns the conditions or restrictions on the processing of personal data of a particular person.[20] In some cases, the concept of privacy has a broader scope than data protection law. We can mention this with the example of a stalker who violates a person's privacy by his behaviour. However, if the stalker does not collect or process the victim's data, he is not covered by the law on personal data protection.[21]

From 1995, the principal legal instrument in EU was Directive 95/46/EC (Data protection Directive), which established a comprehensive data protection system in the EU, though this directive does not apply directly and Member States have a margin of discretion in transposing its provisions. This led to diverse data protection rules across the EU. Modernization was inevitable due to societal changes related to the almost unlimited possibilities from the high-speed internet connection, which makes the exchange of information much easier and faster. [22] The term digital transformation may be defined as 'the change associated with the application of digital technology in all aspects of human society.'[23] The need arose to establish uniform rules for the protection of personal data in the EU. So until the adoption of the GDPR, personal data protection legislation in the Member States was fragmented, and it was the adoption of the GDPR that replaced several national laws in the member states with a common regulation

[18] LAMBERT, P. *Understanding the new European data protection rules*. Boca Raton: CRC Press, Taylor & Francis Group, an Auerbach book, 2020, p. 10-15.
[19] TZANOU, M. *Personal data protection and legal developments in the European Union*. Hershey, PA: Information Science Reference, 2020, p. 1-5.
[20] POLITOU, E. et al. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* [online]. 2018, 20(1) [viewed 3 January 2022], p. 2-3. Available from: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056?login=true
[21] KULK, S. and F. BORGESIUS. Privacy, freedom of expression, and the right to be forgotten in Europe. In: Jules Polonetsky, Omer Tene, Evan Selinger (eds.) *Cambridge Handbook of Consumer Privacy*. 2018, p. 17. Available from: https://www.researchgate.net/publication/320456033_Privacy_freedom_of_expression_and_the_right_to_be_forgotten_in_Europe
[22] *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union, 2018, p. 31.
[23] RHOEN, M. *Big Data, Big Risks, Big Power Shifts: Evaluating the GDPR as an instrument of risk control and power redistribution in the context of big data.* Universiteit Leiden, 2019, p. 4.

defining fundamental rights in the digital society which were applicable throughout the EU. Undoubtedly, it was also accepted because there was increasing pressure from individuals and interest groups for uniform legislation and for strengthening the rights of individuals on the internet.[24]

In 2009, EU Commissioner Viviane Reding announced her intention to amend the Data Protection Directive and the process of a new digital law was launched. She specifically wanted the adjustment to focus on RTBF. She said that 'a unified approach at the EU level will make Europe stronger in promoting high data protection standards globally.'[25] The GDPR is binding and directly applicable to all EU Member States which is typical of this type of secondary law. It came into force on 25 May 2018 after more than two years of legislative vacancy. On this day, all controllers and processors of personal data were obliged to implement the appropriate technical and organizational measures to maintain the confidentiality, integrity and resilience of systems dealing with the processing of personal data. The basic characteristics are the existence of continuity, more precise and detailed regulation of data subjects rights, more elaborate and demanding rules for controllers and processors, and unified independent supervision.[26]

1.2.1 GDPR rights

Personal data must be processed legally, fairly and for legitimate purposes by the institutions of the EU, which is laid down in the GDPR by many other specific rules. The first such rule is the right to be informed, which is connected to the right of transparency in Article 12. The right to be informed is set out in articles 13 and 14 of the GDPR. Individuals need to be clear that their personal data is collected, processed and used, and this information includes transparency concerning all the responsibilities of organizations. This information is therefore required to be easily accessible and comprehensible. Data which has been processed must be clear in terms of the purpose for which it was processed and the identity of the controller. At the same time, individuals are guaranteed information about the risks and rights that come to them in connection with the processing of personal data.[27]

---

[24] GODDARD, M. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research* [online]. 2017 Vol. 59, Issue 6 [viewed January 2022]. Available from: https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050?journalCode=mrea

[25] JONES, M. *Ctrl + Z: the right to be forgotten*. New York: New York University Press, 2016, p. 10.

[26] *Handbook on European data protection law*…, p. 32.

[27] The right to be informed (transparency) (Article 13 & 14 GDPR). *dataprotection.ie* [online]. [viewed 10 February 2021]. Available from: https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-14-gdpr#:~:text=The%20principle%20of%20transparency%20requires,and%20plain%20language%20be%20used

Another right is the right of access provided in Article 15 of the GDPR. This right is very important as it allows entities to exercise other rights as well as to impose fines in the case of incomplete publication. This right gives individuals the right to request a copy of any of their personal data which are processed by controllers as well as other relevant information. The right of access includes the obligation for the EU institution to communicate information on the purposes of processing, the retention period of personal data, their categories and the recipients.[28]

Article 16 of the GDPR allows the right to rectification. It means that

> The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.[29]

It follows that you have the right to rectify your personal data if it is inaccurate or incomplete. It is necessary to rectify any inaccurate personal data that relates to the individual without undue delay and within one month at the most. The right to the restriction of processing imposed in Article 18 gives individuals the opportunity to limit the way an organization uses their personal data, instead of requesting erasure.[30] Another of the enforced rights of the GDPR is the right to data portability in Article 20, which allows entities to obtain data that is retained by the controller. They may use this data for their own purposes, store it for their own use, or pass it on to another administrator.[31]

It is also stipulated that you have the right not to be subject to a decision based solely on automated means, i.e., if this decision has legal effects affecting you or in another significant way.[32] 'The GDPR right to object allows data subjects to object to certain types of data processing and stop a company from continuing to process their personal data. There are only certain situations when a legitimate right to object can be sent to a company.'[33] The most important right which has a really significant influence in digital rights protection is the right to erasure, also known as the right to be forgotten. The RTBF and the right to withdraw consent is the right step to ensure the protection of personal data, however, we cannot take this as

[28] GDPR: Right of Access. *gdpr-info.eu* [online]. [viewed 12 February 2021]. Available from: https://gdpr-info.eu/issues/right-of-access/
[29] Regulation (EU) 2016/679 of the European Parliament…, Article 16.
[30] Ibid., Article 18.
[31] The GDPR for EU institutions: your rights in the digital era. *eda.europa.e*u [online]. [viewed 10 February 2021]. Available from: https://www.eda.europa.eu/docs/default-source/documents/your-rights-in-digital-era---factsheet-1.pdf
[32] Regulation (EU) 2016/679 of the European Parliament…, Article 22.
[33] Ibid., Article 21.

a solution to all problems and exercise these rights in all cases. For this reason, it has been necessary to introduce several comments and guidelines explaining the functioning of the GDPR and, of course, the CJEU's interpretation.[34] In addition, the GDPR established an independent European data protection board to contribute to the uniform application of data protection rules in the EU and to promote cooperation between the data protection authorities of all Member States.[35]

1.2.2 Right to be forgotten

The legal regulation of the RTBF in the legal order can be described as multi-level. One level is the general protection of the right to privacy and the right to the protection of personal data at the level of EU primary law, another level is the RTBF under EU secondary law and the other level relates to the case law of the CJEU. The RTBF in general is conceived as a legal claim, value or interest that is worthy of legal protection. It consists of trying to make information that has already been published private again.[36] This right was not provided for in the Data Protection Directive, however, personal data subjects were given several options to exercise retroactive control over their own information footprint. For example, Article 6 of this Directive stipulates that data must be adequate, published for their purpose, up-to-date and in a form allowing the identification of entities for no longer than is strictly necessary.[37]

Today's internet world makes available a vast amount of easily accessible information that can affect the reputation of those people mentioned. So it is very difficult to move away from the past and remove your name from the digital world.[38] The RTBF as an institute was gradually created in response to the rapid development of modern technologies. The legal predecessor of this right appeared in the English case of AMP in Persons Unknown. In 2008, a British student has her phone stolen containing her nude pictures. The images were copied and uploaded to a social site with her name. Someone alerted the girl and the photos were deleted based on the email. However, the images were bundled into a torrent file and uploaded

---

[34] LINDSAY, D. The "right to be forgotten" is not censorship. *monash.edu* [online]. 2012 [viewed 3 February 2022]. Available from: https://www.monash.edu/news/opinions/the-right-to-be-forgotten-is-not-censorship

[35] BRÄUTIGAM, T. and S. MIETTINEN. *Data protection, Privacy and European Regulation in the Digital age.* Helsinki: Unigrafia, 2016, p. 63-64.

[36] JONES, M. It's About Time: Privacy, Information Lifecycles, and the Right to Be Forgotten. *Stanford Technology Law Review* [online]. 2013, vol. 16, no. 2 [viewed 10 February 2021]. p. 101-154. Available from: http://ssrn.com/abstract=2154374

[37] AUSLOOS, J. The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review* [online]. 2012 [viewed 10 February 2021], p. 149. Available from: https://is.muni.cz/el/law/jaro2019/SOC022/um/59943709/The__Right_to_be_Forgotten__-_Worth_remembering.pdf

[38] RUSTAD, M. and S. KULEVSKA. Reconceptualizing the Right to be Forgotten to enable Transatlantic Data Flow. *Harvard Journal of Law & Technology* [online]. 2015, 28(2) [viewed 2 February 2022], p. 349-352. Available from: http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech349.pdf

to The Pirate Bay. The girl was then blackmailed. The girl used various legal means to remove the photos, first filing a notice with Google to stop distributing the images, then a court order to the High Court in England and Wales to prevent the transfer of the data under the applicant's right to privacy under Article 8 of the ECHR.[39] The damage caused to private life prevails and therefore the publication of images through any medium should be prevented. However, RTBF does not use privacy, instead it is the application of data protection law.[40]

The RTBF first appeared and was stated in the case law of the CJEU in Google Spain in 2014. This was the first case that directly applies existing data protection principles to the internet and permits the erasure of search data. It also emerged from this judgment that fundamental rights had begun to take precedence over economic interests. Thus, corporations have a greater responsibility for human rights which has come to the fore thanks to the digital age.[41] But the Court did not explicitly grant such a right. The ruling enshrined 'right to forget' and defended the position of the right to forget against the general public right to information.[42] This right gives individuals control over their personal data and streamlines the consent regime. One of the definitions is 'The right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.'[43] However, we now proceed from Article 17 of the GDPR, which provides us with right to erasure or RTBF. Article 17 states that the entity has the right to delete personal data from the controller without undue delay, but only such data that concern him or her. In order for an individual to exercise this right and the controller to delete individual data, at least one of the conditions must be met, such as the purpose for which the personal data were disclosed is no longer necessary, the data subject objects to the processing, or personal data are being processed illegally.[44]

As mentioned in the previous chapter, the RTBF is also referred to as right to erasure. For this reason, experts view this right as two concepts, which, although materially having the same content, differ in situations within their application. The right to erasure provides entities with the opportunity to invoke the deletion of their personal data if the conditions

[39] Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome, 1950, Article 8.
[40] GUADAMUZ, A. Developing a Right to be Forgotten…
[41] RAZMETAEVA, Y. The Right to Be Forgotten in the European Perspective. *TalTech Journal of European Studies* [online]. 2020, Vol. 10, No.1 [viewed 10 March 2022], p. 63. Available from: https://sciendo.com/article/10.1515/bjes-2020-0004
[42] KAMPARK, B. To Find or be Forgotten: Global Tensions on the Right to Erasure and Internet Governance. *Journal of Global Faultlines* [online]. 2015, 2(2) [viewed 2 February 2022], p. 1-3. Available from: https://www.jstor.org/stable/10.13169/jglobfaul.2.2.0001#metadata_info_tab_contents
[43] AUSLOOS, J. The 'Right to be Forgotten' – Worth remembering?..., p. 149.
[44] Regulation (EU) 2016/679 of the European Parliament…, Article 17.

stipulated by law are met. The right to erasure is thus very closely linked to the fundamental right of the protection of personal data. The RTBF, in contrast to the right to erasure, is meant in the sense of the protection of personal rights, i.e. the protection of dignity or reputation. It can be interpreted as the right of an individual not to be associated with a certain true event or a fact which, as a result of the passage of time, has lost its informativeness. This right is therefore linked to the protection of human privacy.[45]

This right gives EU citizens the opportunity to ask search engines to remove specific listings from search results that lead to content that may be inappropriate, defamatory or irrelevant. If the request for data deletion is rejected, as a system of checks and balances, the user has the right to lodge a complaint with his or her data protection authority.[46] In the context of the protection of personal data and the RTBF, it is necessary to define the boundaries of the right to privacy and the protection of personal data and its possible limitations. It is necessary to know that information self-determination is not the same as privacy, although in many cases they may interact. The RTBF usually contains information that may in some way violate the basis of the right to privacy and prevent the protection of personal data.[47] The CJEU must therefore seek to strike a balance between these rights.

The adoption of the GDPR and the RTBF provisions have widened the gap between the US and EU in the relationship between the right to privacy and freedom of expression. The RTBF is only valid in the Member States of the EU and is considered by many American legislators to be a violation of freedom of expression. According to them, it serves to bury information, favours censorship and hinders freedom of information.[48] This is also due to the cultural environment of these continents, where there is a history of privacy regulations in Europe, while in the US privacy issues have primarily been addressed indirectly through market-based approaches and voluntary codes of conduct.[49] The EU clearly favours the protection of individuals' personal data, which affects the RTBF, while the public's right to information prevails in the historical development of US law, where this right is enshrined in the First Amendment. For this reason, the RTBF may even be perceived as unconstitutional.

---

[45] AUSLOOS, J. The 'Right to be Forgotten' – Worth remembering?...,p. 149.
[46] NEVILLE, A. Is it a Human Right to be Forgotten? Conceptualizing the World View. *Santa Clara Journal of International Law* [online]. 2017, 15(2) [viewed 2 February 2022], p. 162. Available from: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1221&context=scujil
[47] KULK, S. and F. BORGESIUS. Privacy, freedom of expression, and the right to be forgotten in Europe…, p. 11-13.
[48] GUADAMUZ, A. Developing a Right to be Forgotten…
[49] STAINFORTH, E. Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union. *Journals.sagepub* [online]. 2021 [viewed 2 February 2022], p. 8. Available from: https://journals.sagepub.com/doi/pdf/10.1177/17506980211044707

It is also typical of the US to place more emphasis on freedom of speech than on privacy.[50] This follows from the fact that the right to respect for private life in the US 'finds no explicit direct protection in the US Federal Constitution'[51]

[50] BENNET, S. The "Right to Be Forgotten": Reconciling EU and US Perspectives. *Berkeley Journal of International Law* [online]. 2012 [viewed 2 February 2022], p. 169. Available from: https://lawcat.berkeley.edu/record/1125027

[51] WERRO, F. Balancing the Freedom of Expression Against the General Right to Privacy: The European Approach vs. the United State's Approach. In: Franz Werro (ed.). *The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia.* Cham: Springer, 2020, p. 4.

2 Right to be forgotten in the case law of the CJEU

In this chapter we come to the case law of the CJEU itself, which is consider to be one of the most important sources of digital fundamental rights and fills gaps in EU law. The RTBF has become more widely discussed thanks to the decision-making practice of this Court. I will now turn to the judgments concerning this right which first mentioned, established, deepened and shaped it in its present form. Thanks to modernization and digitization there have been more cases where previously printed media and newspapers have been digitized and the data contained in them have become readily available online to the public, even in cases where this data was not relevant at all. The protection of personal data may conflict with other rights; for example, RTBF is opposed to the right of the public to information. Judges will decide which of the variants will be preferred when performing the proportionality test in a specific case.

Everything began with the judgment of Google Spain, which first mentioned the RTBF. Then came other important judgments, which concretized and regulated this right. Its interpretation and implementation have in many cases caused worrying tensions over the right to freedom of expression and information. Judgments concretizing this right are often widely analysed, as experts find many grey areas that could have an impact on human rights. It is also often stated that the decisions puts power primarily in the hands of search engines to decide what content will be discovered in the online world.[52] According to Post:

> Google Spain is ultimately an ambiguous and opaque decision because it is uncertain whether the CJEU sought to preserve the right of data subjects to control personal information or instead to safeguard the dignity of human beings. We do not know whether the object of the decision is data privacy or dignitary privacy.[53]

Although the RTBF is the solution to many problems in the digital world, this institute is not enforceable in all cases. The problem may arise, for example, in the area of data anonymization, where controllers and processors of personal data may oppose the deletion of personal data on the grounds that the data are already anonymized.[54] Another problem may be the case when an individual requests the deletion of personal information on one website, which, however, has already been copied to another page and further processed, or has been

[52] EU Court decides on two major "right to be forgotten" cases: there are no winners here. *accessnow.org* [online]. 23 October 2019 [viewed 6 April 2021]. Available from: https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/

[53] POST, R. Data privacy and dignitary privacy: Google Spain, the Right to be forgotten, and the construction of the public sphere…, p. 994.

[54] *Mosley v. the United Kingdom*, ECtHR, Application No. 48009/08, Judgement, 10 May 2011.

anonymized.[55] Another problem is that the internet knows no borders and the EU can only regulate the RTBF in the territory of its Member States. The best solution would be a joint agreement between the EU and the US, as the different approach and non-existence of the RTBF in the US have a negative impact on law enforcement in the EU. The challenge for this right in the future is to make it known to the general public, as EU citizens' awareness of the existence and exercise of this right is very limited.[56]

2.1 Google Spain

The judgment in Case C-131/12, known as Google Spain, concerns the proceedings brought by Google against the AEPD and Mario Costeja González in 2012. At that time, Directive 95/46/EC applied in the EU. This directive provided a framework for the regulation and processing of personal data protection in the EU. However, the requirements of this directive have been implemented separately in each country, with data protection laws and regulations varying slightly from country to country.[57] The directive defined personal data in Article 26 as 'any information concerning an identified or identifiable person'.[58]

In 2009, Mr González turned to La Vanguardia and complained that if his name was entered into Google.com, there was a link to the newspaper's online litigation pages. In 1998, two articles were published by those Spanish newspapers concerning an attachment and garnishment action against Mr González. His assets were the subject of a public auction in the 1990s because he owed social security payments and this information was published in the daily press in accordance with Spanish law in order to secure a larger number of participants at the public auction. Mr González requested the removal of this information as the proceedings had been closed several years ago and there was no outstanding claim against him. The newspaper did not comply with this request and substantiated the publication of the article by order of the Spanish Ministry of Labour and Social Affairs.[59]

Mr González approached Google Spain a year later, again demanding the removal of the link associated with his name. Google's search engine works on the principle called 'googlebot'. This function is used to systematically browse the internet and the websites visited

[55] AUSLOOS, J. The 'Right to be Forgotten' – Worth remembering?..., p. 146.
[56] MACH, Martin. Právo být zapomenut jako reakce na vývoj informačních technologií. *Právník* [online]. 2021, [viewed 8 February 2022], p. 605-608. Available from: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2021/7/7_Mach_597-609_7_2021.pdf
[57] EU Data Protection Directive. *uk.practicallaw.thomsonreuters.com* [online]. 1 January 2019 [viewed 10 April 2021]. Available from: https://uk.practicallaw.thomsonreuters.com/6-501-7455?transitionType=Default&contextData=(sc.Default)&firstPage=true
[58] Directive 95/46/EC…, Article 26.
[59] KULK, S. and F. BORGESIUS. Privacy, freedom of expression…, p. 17.

and then send it a copy of the subpage visited. It is thus switched from one source website to another on the basis of so-called hypertext links between pages. These copies of the source web pages are then analysed by a system of 'web crawlers' for examining and indexing the content of individual web pages.[60] Following another failed attempt, Mr González filed a complaint before Spain's Data Protection Agency against the newspaper, Google Spain, and Google Inc. While acknowledging the complaint against Google and its subsidiary Google Spain, the agency dismissed the lawsuit against the newspaper because the publication of the article was based on a government regulation, as the newspaper itself had already mentioned. Internet search engines are governed by privacy laws and can therefore be required to remove information that may infringe on the privacy of individuals. Google and its subsidiary in Spain appealed against this decision.[61]

The National High Court of Spain decided to stay the proceeding, stating that it was necessary to examine the obligations incumbent on search engine operators in order to protect the personal data of data subjects who do not wish certain information published on third-party websites to be searched indefinitely. The answer depends on the way in which Directive 95/46 is interpreted in the light of those technologies which have emerged since its publication. This court turned to the CJEU during a preliminary ruling.[62] Their questions mainly related to the territorial scope of Directive 95/46 and the interpretation of Article 4 as to whether Google could be held liable as a data controller. Furthermore, the CJEU was asked to comment on whether the right to delete and the right to object enshrined in the directive could be extended in order to request the removal of data from an internet search engine.[63]

The question of whether the Google search engine could be classified as a processor of personal data was answered in the affirmative, as the company's activities concern both the collection and publication of personal data and are therefore considered to be processors for the purposes within the meaning of Article 2b) Directive 95/46/EC. The directive defines processing as

> any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or

[60] Opinion of Advocate General delivered on 25 June 2013 (1), Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González
[61] POST, R. Data privacy and dignitary privacy: Google Spain…, p. 995 - 997.
[62] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. C-131/12, CJEU, Judgment of the Court (Grand Chamber), 13 May 2014, para 19.
[63] Ibid., para 20.

alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[64]

According to the decision of the Court, Google is also considered to be a controller as it determines the purposes and means of processing personal data according to Art. 2 d) of the directive. On the question of whether from a geographical point of view the directive affects the present case, the CJEU referred to Art. 4 (1) (a) of Directive 95/46, which provided that it was sufficient for the processing to take place in the course of the controller's business, which was the case here. Google Spain has defended itself as a subsidiary of Google Inc., a global search engine operator, and its profits come from advertising messages attached to search results. The purpose of Google Spain's activities is to promote local advertising sales and the company has argued that it does not fall within the Spanish jurisdiction, as the processing of personal data itself took place outside Spain and is not carried out by Google Spain.[65] EU rules apply to search engine operators if they have a subsidiary in a Member State, even if the physical server of the data processing company is located outside the EU.[66]

However, the most important decision in this case concerned the deletion of data of specific persons, which, although previously published in accordance with the law, have over time become incompatible with the directive and are no longer necessary for the purposes for which they were previously processed.[67] 'The point of data privacy is to protect the data subject's control over his personal information.'[68] However, it was emphasized that the right to request deletion of data may lapse if there is an overriding public interest in the information. The right of internet users to access personal information is therefore respected on the basis of the nature of the information and the public interest in knowing that information, in particular according to the role played by the data subject in public life.[69]

The ruling of the CJEU in this case was ground breaking as it stated that EU citizens had the right to request that commercial search firms which gather inaccurate or irrelevant

[64] Directive 95/46/EC…,Article 2 (b).
[65] IGLEZAKIS, I. The Right To Be Forgotten in the Google Spain Case (case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet? *Paper presented at the 4th International Conference on Information Law* [online]. 27 July 2014 [viewed 9 February 2022], p. 8. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323
[66] GSCHNELL, M. and M. WEIDEMAN. A critical study of "The Right to be forgotten" – a Google case Study. *Working paper* [online]. Munich University of Applied Science, Munich, 2014 [viewed 9 January 2022], p. 3. Available from: https://www.researchgate.net/publication/324542829_A_critical_study_of_The_right_to_be_forgotten_-_a_Google_case_Study_0154
[67] POST, R. Data privacy and dignitary privacy…, p. 997-1000
[68] Ibid., p. 998.
[69] Google Spain…, para 97.

personal information should remove links to this private information. On the other hand, the request to delete a newspaper article from the website was rejected and criticised as it would violate the freedom of the press. The scope of the right in this case has not yet been fully defined and its applicability to various types of data on the internet has not been resolved.[70] However, the decision only applies to internet search engines and the right to delete links to data subjects' information in the list of results displayed by searching for a specific name. As a result, the internet search service provider is obliged to consult the provider of the website on which the personal data is published and to assess the privacy regarding the facts related to the dissemination of personal data. The provider of these services must take responsibility for the processing of the personal data it takes over.[71] According to some experts, the CJEU did little to substantiate its allegations in that decision and refers in particular to the need to maintain a high level of privacy. The CJEU also prioritises the right to personal data protection, thus conflicting with the right to freedom of expression.[72] The decision was also criticized for introducing a kind of automated rule whereby the interests of the individual are always higher than the economic interests of the data controller. This decision is considered to guarantee the RTBF, which follows from Article 7 and Article 8 of the CFR. [73]

Another impact of this judgment was the publication of a form by Google that allows individuals to request the removal of search results.[74] An Advisory Council to Google on the RTBF was set up to deal with this right and its incorporation into practice. This consists of independent experts who serve as advisors to Google on how to strike a balance between an individual's right to privacy and the public's interest in accessing information. In 2015, the Council published its recommendations in a final report and held 7 consultations in various European cities. [75] For example, experts established 4 basic criteria recommending that Google evaluate cancellation requests: Data Subject's Role in Public Life, Nature of the Information,

[70] GSCHNELL, M. and M. WEIDEMAN. A critical study of "The Right to be forgotten"…, p. 3.
[71] IGLEZAKIS, I. The Right To Be Forgotten…, p. 12.
[72] LYNSKEY, O. Rising like a Phoenix: The 'Right to be Forgotten' before the ECJ. *europeanlawblog.eu* [online]. 13 May 2014 [viewed 19 February 2022]. Available from: https://europeanlawblog.eu/2014/05/13/rising-like-a-phoenix-the-right-to-be-forgotten-before-the-ecj/
[73] BUNN, A. The Curious Case of the Right to Be Forgotten. *Computer Law & Security Review* [online]. 2015, no. 3 [viewed 20 April 2021], p. 344. Available from: https://www.sciencedirect.com/science/article/pii/S0267364915000606
[74] Personal Information Removal Request Form. *google.com* [online]. [viewed 20 April 2021]. Available from: https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&hl=en
[75] How should one person's right to be forgotten be balanced with the public's right to information? *archive.google.com* [online]. [viewed 20 April 2021]. Available from: https://archive.google.com/advisorycouncil/

Source and Time.[76] Interestingly, in the year the Google Spain decision was issued, from January to July Google received over 91,000 removal requests for more than 328,000 URL's, approved more than 50% of them, rejected more than 30% and asked for more information for another 15% of requests. In the following years, the number of applications fell sharply and more recently the number has been stagnating.[77]

2.2 Camera di Commercio v Manni

In this case, Mr Manni sought to rely on a previous decision in the case of RTBF in Google Spain. Mr Manni won a contract to build a tourist complex in Italy but was unable to sell the property in the complex because there was information in the commercial register that he was the trustee of another company which went bankrupt in 1992 and was liquidated in 2005. Therefore, he brought an action against the Lecce Chamber of Commerce in 2007. In 2011, a court in Lecce upheld the lawsuit, ordering the Lecce Chamber of Commerce to anonymize but not remove information concerning Mr Manni. The court argued that if there is no public interest, the records should not be permanent. However, Italian law did not provide for a retention period in the commercial register.[78]

The Lecce Chamber of Commerce appealed this decision directly to the Italian Supreme Court pursuant to the Italian Data Protection Code, as the public interest is demonstrated by the fact that the data helped to increase legal certainty. However, the Supreme Court recognized the RTBF as a fundamental tool for protecting personal identity. The court referred a question to the CJEU whether in the absence of any legal rule, the protection of personal data gives the data subject the right to obtain the cancellation or anonymization of his or her data published in the companies' register after a certain period of time. The question in this case was whether it is possible to request a natural person to delete personal data from the Commercial Register after a certain period of liquidation and whether the principle of keeping personal information only for as long as necessary under Directive 95/46/EC takes precedence over the principle of 'unlimited duration and indefinite circle of recipients of information published in the public register' under Directive 68/151.[79]

---

[76] The Advisory Council to Google on the Right to be Forgotten. *static.googleusercontent.com* [online]. 6 February 2015 [viewed 9 February 2022]. Available from: https://static.googleusercontent.com/media/archive.google.com/cs//advisorycouncil/advisement/advisory-report.pdf

[77] IGLEZAKIS, I. The Right To Be Forgotten…, p. 5.

[78] CARAVA, E. Personal Data Kept in Companies Registers: The Denial of the Right to Be Forgotten. *Eur. Data Prot. L. Rev.* [online]. 2017 [viewed 11 February 2022], p. 287. Available from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=52&id=&page=

[79] *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni*, C-398/15, Judgment of the Court (Second Chamber), 9 March 2017, para 29.

On the basis of Article 2 (1) of Directive 68/151, the Court first ruled that the persons empowered to act on behalf of the company and the appointed liquidators must be published in the commercial register.[80] The processing of personal data also occurs in the case of their publication and therefore the principles concerning such processing pursuant to Articles 6 and 7 of Directive 95/46/EC must be observed. The erasure of such information must be decided on the basis of the purpose of the processing, which is based, in accordance with Directive 68/151, primarily on the protection of third parties entering into or already in economic relations. If such information is not disclosed, individuals should not be able to verify the credibility of the company.[81]

The CJEU has established the freedom of Member States to provide for exceptions to delete personal data from the public register and does not consider Mr Manni to be a relevant reason for deletion in the event of a reduced sale.[82] This decision concerns the addition of the possibility of exercising the RTBF, more specifically in the area of deletion of personal data from the public register. The CJEU has ruled that the Member States should decide on the RTBF in each case individually. For overriding legitimate reasons, access to information for third parties may be restricted after a sufficient period of time has elapsed. [83]

2.3 Judgments in GC and Others and Google v CNIL

Although since the adoption of the GDPR the RTBF has been enshrined in this regulation, some important aspects of this right have remained unanswered. Therefore, in 2019, the CJEU delivered two judgments supplementing previous case law in two basic cases. The case of GC and Others is clarified by the processing of sensitive data by search engine operators and the removal of references to that data, and the judgment of Google v CNIL defines the territorial scope of the RTBF. In this case, the CJEU decided between recognizing the RTBF at the global level and increasing protection or recognizing this right as non-universal, with an emphasis on the digital sovereignty of states.[84] These judgments also provide an interpretation for a better

[80] Ibid., para 32.
[81] Ibid., para 50.
[82] Ibid., para 63.
[83] BOWDEN, D. CJEU rules director of failed company has no right to be forgotten at Companies House. *ewriter.eu.* [online]. 9 March 2017 [viewed 15 April 2021], p.6. Available from: http://www.ewriter.eu/articles/Manni.pdf
[84] HAMULAK, O. and H. KOCHARYAN. The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union. *Researchgate.net* [online]. 2021 [viewed 10 March 2022], p.202. Available from: https://www.researchgate.net/publication/357430418_The_Global_Reach_of_the_Right_to_be_Forgotten_through_the_Lenses_of_the_Court_of_Justice_of_the_European_Union

understanding of the relationship between the RTBF and freedom of information.[85] 'This decision has to be understood as an act which brings the processing of sensitive data by search engines out of the grey area caused by the Court's decision in Google Spain and into the sphere of legality.'[86]

2.3.1 GC and Others

Four applicants independently requested Google to delete links to certain websites that contained allegedly sensitive personal information, in accordance with Article 8 of now replaced Directive 95/46/EC. This included the deletion of a satirical photomontage of a complainant with a politician or the identification of a worker in relation to the Church of Scientology. Google rejected these requests, the applicants brought their complaints before the French data protection authority (CNIL), which refused to serve formal notice on Google to carry out the de-referencing requested. This was followed by a complaint to the Council of State, which referred questions to the CJEU concerning the applicability of the ban on the processing of sensitive data in search engines and the removal of their link.[87]

First, the CJEU was required to determine whether internet search engine operators are prohibited from processing sensitive personal data under Article 8 (1) and (5) of Directive 95/46/EC, as well as other personal data controllers.[88] Furthermore, the Court wanted to clarify whether the ban on the processing of sensitive data necessarily leads to the immediate request for deletion or whether operators may refuse deletion on the basis of the exceptions to the ban on processing personal data under Article 8 (2) of this directive. They can therefore benefit from the exemptions provided for in Article 9 of the directive, i.e. processing for journalistic, artistic and literary purposes.[89] Other questions concerned the obligations of the operator in the case of finding out that personal data have been processed illegally and whether they are obliged to delete information that does not correspond to the current state.[90]

The Court replied that the prohibition on the processing of personal data of special categories also applies to the search engine operator under its responsibility under the supervision of the competent national authorities at the request of the data subject.[91] Article

---

[85] GLOBOCNIK, J. The Right to Be Forgotten is Taking Shape: CJEU Judgments in *GC and Others* (C-136/17) and *Google v CNIL* (C-507/17). *GRUR International* [online]. 2020, vol.69, issue 4 [viewed 15 April 2021], p. 380-388. Available from: https://academic.oup.com/grurint/article/69/4/380/5732807

[86] Ibid., p. 380

[87] Ibid., p. 381.

[88] Opinion of Advocate General Szpunar delivered on 10 January 2019 (1), Case C-136/17, para 39.

[89] Ibid., para 60.

[90] *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17, Judgment of the Court (Grand Chamber), 24 September 2019, para 32.

[91] Ibid., para 48.

8 of Directive 95/46/EC reads 'Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.'[92] These prohibitions applied to all types of processing a special category of data performed by search engines. It was emphasizes that Google was responsible

> not because personal data referred to in those provisions appear on a web page published by a third party but because of the referencing of that page and in particular the display of the link to that web page in the list of results presented to internet users following a search on the basis of an individual's name, since such a display of the link in such a list is liable significantly to affect the data subject's fundamental rights to privacy and to the protection of the personal data relating to him.[93]

Then it was decided that a search engine operator must only verify the lawfulness of its processing of sensitive data ex post, i.e., upon receiving a request for de-referencing. The Court then returned to the judgment of Google Spain and to the fact that the rights of data subjects may prevail over freedom of information, however, the balance between these rights must be assessed in each case on the basis of

- 'the nature of the information in question and its sensitivity for the data subject's private life; and
- the interest of the public having that information, an interest "which may vary, in particular, according to the role played by the data subject in public life.'[94]

It was confirmed that a similar balance test should apply to the processing of data on convicted offenders.

2.3.2 Google v CNIL

The French Privacy Authority has called on Google to remove links to third-party privacy sites from all national versions. Until now, if the information was deleted at the request of a person, it would disappear only from the home domain and other European domains. Google has refused to remove links to list searches that contain personal information that was harmful to individuals from Google domains outside the EU.[95] They suggested complementing this

[92] Directive 95/46/EC…, Article 8.
[93] *GC and others*…, para 46.
[94] NADEGE, M. and N. SHABESTARI. The right to be forgotten: the CJEU sides with Google in two landmark cases. *Dataprotectionreport.com* [online]. 9 October 2019 [viewed 8 May 2021]. Available from: https://www.dataprotectionreport.com/2019/10/the-right-to-be-forgotten-the-cjeu-sides-with-google-in-two-landmark-cases/
[95] CNIL orders Google to apply delisting on all domain names of these archengine. *cnil.fr* [online]. 12 June 2015 [viewed 8 May 2021]. Available from: https://www.cnil.fr/fr/node/15790

solution with geo-blocking. It introduces measures for domains accessible from EU countries. Once a link to a page with the applicant's personal data has been removed from a specific country, it will not be possible to display it on non-European Google domains if the user searches for this information in the country where the link removal request came from.[96] Therefore, CNIL did not consider this solution to be sufficient. The case was referred to the CJEU by the French Council of State. Google has also changed its search engine to automatically redirect Internet users to the national version that matches the location of the search.[97]

The CJEU held that Google and other search engines are required to delist search results from domains within the EU, but not globally. That judgment ruled that the RTBF has limited territorial scope. Nevertheless, operators should use and take measures that effectively prevent and, in particular, reduce the chances of internet search engine users searching for 'forgotten' links. The RTBF shall apply only to operations carried out in the Member States, in particular when exercised against a controller with multinational or global operations. Article 17 of the GDPR, Articles 12 and 14 of the Data Protection Directive, as well as the judgment C-131/12 which first recognized the RTBF, were examined. According to the CJEU, the right to the protection of personal data is not absolute and should be assessed in relation to its function in society. In addition, the principle of proportionality should be applied. This judgment therefore leads to differences between countries depending on this right, the right to privacy and the right to freedom of expression.[98]

[96] FLEISCHER, P. Adapting our approach to the European right to beforgotten. *blog.google.com* [online]. 4 March 2016, [viewed 8 May 2021]. Available from: https://www.blog.google/around-the-globe/google-europe/adapting-our-approach-to-european-rig/
[97] GLOBOCNIK, J. The Right to be forgotten…, p. 380-388.
[98] SAMONTE, M. Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law. *europeanlawblog.eu.* [online]. 29 October 2019 [viewed 11 May 2021]. Available from: https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law

3 Other important CJEU judgments in digital rights matters

In this chapter, I will focus on other cases that have helped to improve the protection of human rights in the digital sphere. These judgments were especially important point in the functioning of internet service providers, document sharing and data retention. It is in these cases that IP addresses are stored, which are now also considered as personal data. The nature of the IP address as personal data was not entirely clear before and the CJEU has been working on this issue for a long time. By personal data we mean all information about an identified or identifiable natural person, and since the IP address can be used to identify the user, the IP address is also included among the personal data.[99] The CJEU declared a long-term view on the issue of dynamic IP addresses, which in conjunction with other data may represent personal data, which culminated in an explicit mention of network identifiers within the definition of personal data in the GDPR. I will analyse further details in the individual judgments, which I have arranged on the basis of the time sequence, i.e. from the 'oldest' to the 'newest'. I will deal with those judgments which are considered the most important and which have greatly affected the functioning of the digital world.

3.1 'Scarlet Extended'

The 'Scarlet Extended' judgment refers to a dispute between an internet connection provider and a management organization representing authors, and concerns the imposition of an obligation on the internet connection provider to introduce a system for filtering all incoming and outgoing electronic communications. SABAM, a Belgian management company representing the authors and composers of musical works, brought proceedings against Scarlet, an internet service provider, because users of Scarlet's internet services were downloading copyrighted works in SABAM's catalogue without authorization by using peer-to-peer software.[100] Peer-to-peer networks are based on transparent and independent file sharing based on the file search and download function.[101] SABAM also demanded an end to Scarlet's infringement by 'blocking, or making it impossible for its customers to send or receive in any

[99] GDPR, Article 4(1).
[100] KEYDER, V. Introductory note to the European Court of Justice: Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs, Ed Editeurs SCRL (SABAM). *International Legal Materials* [online]. 2012, vol. 51 [viewed 11 May 2021], pp.382-392. Available from: https://www.jstor.org/stable/10.5305/intelegamate.51.2.0382?casa_token=sGecAvFaIKsAAAAA%3A2Yvi7Ph1IrnPGwQILlmc7m71pG0nAO3PgjHftSTn-LOBKIBE-wOovfn-DQON-axaqs5az1lEpPaTEomQdYFkTgL-unIVuF4OgTHQyE7NrdtELBHGkD4&seq=1#metadata_info_tab_contents
[101] *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, Judgment of the Court (Third Chamber), 24 November 2011, para 17.

way, files containing a musical work using peer-to-peer software without the permission of the rightholders, on pain of a periodic penalty.'[102]

The court of first instance in Brussels found copyright infringement but first appointed an expert on whether it was possible to implement the technical solutions proposed by SABAM.[103] Following the consultation Scarlet was ordered to take measures to block illegal file sharing by customers.[104] Scarlet appealed against that decision, alleging that such requirements could not be met. In its view, that was contrary to Article 21 of the Law of 11 March 2003 on certain legal aspects of information society services, which transposes Article 15 of Directive 2000/31 into national law.[105] It also stated that the filtering system is a breach of the provisions of EU law on the protection of personal data, as it means the processing of IP addresses which are personal data.[106] The Court of Appeals referred the case to the CJEU for a preliminary ruling. The Court wanted to clarify whether it was in accordance with EU law to issue an injunction against internet intermediaries by a national court if their services are used by third parties to infringe copyright and whether the company can be forced to install a filtering system to block illegal file sharing.[107]

It is possible to identify a specific user on the basis of their IP address, then this constitutes personal data as understood in Article 2 (a) of Directive 95/46/EC. Although the protection of intellectual property rights is enshrined in CFR, it does not follow that such a right is inviolable. The Court stated that in order to prevent any infringement of intellectual property rights, the order would impose an obligation on Scarlet to actively monitor all of the data of each of its customers and therefore an obligation of general supervision. However, this is incompatible with the e-commerce directive and is therefore contrary to fundamental rights.[108] The order would also continue to interfere with Scarlet's business, as it would have to set up a permanent computer system at its own expense.[109] The CJEU ruled that such a measure was incompatible with Directive 2000/31, which in Article 15 (1) prohibits the imposition of an obligation on ISPs to carry out general checks on information transmitted by its network and the protection of personal data under the CFR.[110] The CJEU said that the protection of intellectual property rights is not an absolute right and it is necessary to compare it with the protection of other rights.

[102] Ibid., para 20.
[103] Ibid., para 21.
[104] Ibid., para 23.
[105] Ibid., para 24-25.
[106] Ibid., para 26.
[107] Ibid., para 28 (1).
[108] KEYDER, V. Introductory note to the European…
[109] *Scarlet extended*,…, para 48.
[110] Ibid., para 40.

Subsequently, it is necessary to find an appropriate balance between the rights and to measure the rights in terms of proportionality. This judgment also defined in more detail the boundary between the general and the specific duty of supervision.[111]

3.2 Digital Rights Ireland

This joined judgment concerned preliminary questions on the validity of certain provisions of Directive 2006/24/EC on data retention precisely in the context of Articles 7, 8 and 11 of the CFR. The Data Retention Directive required communication service providers to retain certain types of personal data for the purpose of detecting and prosecuting serious criminal offenses. It should be noted that the Data Retention Directive was adopted at a time of heightened risk perception during the terrorist attacks on Madrid and London in 2004-2005. Digitization largely affects our communication capabilities, which are increasingly turning into communication via mobile phones and social media. This leaves a trail that can be useful in criminal proceedings and can affect our private lives. This case law therefore deals with laws that use communication data, which must be in balance with security benefits but also with respect for fundamental rights.[112]

3.2.1 The facts of the cases

Firstly, I will introduce case C-293/12. Digital Rights Ireland is civil-rights lobby group in Ireland, which brought an action against the retention of telecommunications data before the Irish High Court. Telecommunications data were provided by the Criminal Justice (Terrorist Offences) Act 2005. According to Digital Rights Ireland, the national police service of the Republic of Ireland gained access to classified data under that law without investigating a specific third act. It claimed that the mobile phone, registered in June 2006 and which had been used since that date, called into question the legality of national legislative and administrative measures concerning the retention of electronic communications data. Digital Rights Ireland required the Court to rule on the invalidity of the Data Retention Directive and Part Seven of the Criminal Justice Act 2005 as it considered this to be

[111] Scarlet Extended SA v. SABAM. *globalfreedomofexpression.columbia.edu* [online]. [viewed 15 February 2022]. Available from: https://globalfreedomofexpression.columbia.edu/cases/scarlet-extended-sa-v-sabam/

[112] GRANGER, M. and K. IRION. The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection. *European Law review* [online]. 2014 [viewed 15 February 2022], p. 835. Available from: https://pure.uva.nl/ws/files/65990842/The_Court_of_Justice_and_The_Data_Retention_Directive_in_Digital_Rights_Ireland_Kristina_Irion_and_Marie_Pierre_Granger.pdf

incompatible with the CFR.[113] In order to rule on the illegality of the national provision, the High Court asked the CJEU to review the directive and its compatibility with the CFR.[114]

Another case, C-594/12, concerned a request made by the Austrian Constitutional Court relating to constitutional actions brought before that court by the Government of the Province of Carinthia and by Mr Seitlinger and others regarding the compatibility with the Federal Constitution of the law transposing the Data Retention Directive into Austrian national law. The appellants sought the annulment of Article 102a of the Austrian Telecommunications Law implementing the directive on the grounds of a breach of the fundamental right to the protection of personal data. This was mainly because the law allows for the retention of people's data over a long period and, therefore, these people are exposed to the risk of authorities investigating their data and accessing content and information about their private lives.[115] Similarly to the Irish court, the Austrian court asked whether the Data Retention Directive is valid in light of Articles 7, 8 and 11 of the CFR.[116]

3.2.2 Joined Judgment

The CJEU acknowledged the fight against terrorism as a serious activity of general interest and noted the right to security protected by Article 6 of the CFR. The Data Retention Directive therefore met the objective of general interest, but the need arose to consider proportionality to other rights.[117] First of all, the CJEU had to assess whether the retention of data under this directive fell under articles 7 and 8 of the CFR. The retention of data directly and specifically affects the private lives of individuals and is therefore guaranteed by Article 7 of the CFR.[118] At the same time, data retention also falls under Article 8, as it constitutes the processing of personal data within the meaning of this article.[119] The Court said that the amount of data covered by the directive can very specifically draw conclusions from people's lives and give the authorities access to everyday data.[120] The directive provided for

[113] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* C-293/12, C-594/12, Judgment of the Court (Grand Chamber), 8 April 2014, para 17.
[114] Ibid., para 18.
[115] Ibid., para 19.
[116] Ibid., para 20.
[117] MURPHY, M. "Data retention in the aftermath of Digital Rights Ireland and Seitlinger." *researchgate.net* [online]. 2014 [viewed 15 February 2022], p. 3. Available from: https://www.researchgate.net/publication/291787781_"Data_retention_in_the_aftermath_of_Digital_Rights_Ireland_and_Seitlinger"
[118] *Digital Rights Ireland Ltd…,* para 26-28.
[119] Ibid., para 29.
[120] GUILD, S. and S. CARRERA. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive Elspeth Guild and Sergio Carrera. *Paper in Liberty and Security in Europe* [online]. 2014 [viewed 15 February 2022], p. 5. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901

an interference with the right to respect for private and family life. The essence of the fundamental right in Article 7 of the CFR was maintained, as the directive did not allow the content of electronic communications to be read directly.[121] It was noted that interference with the right to privacy and the protection of personal data had be kept to the minimum necessary, in accordance with the case law. The directive also allowed Member States to adopt a retention period of between 6 and 24 months, regardless of whether this was strictly necessary given the objective criteria.[122]

The judges agreed that the data retention obligation of the directive presupposes interference with the right to privacy and at the same time, by providing for the processing of personal data, it also interfered with the protection of personal data. These interventions have been described as extensive and serious, which can cause people to feel constantly monitored.[123] The CJEU ruled that the directive is invalid on the grounds that it has exceeded the limits of the principle of proportionality in relation to certain provisions of the CFR. The Court repealed this directive on 8 April 2014. In essence, the CJEU agreed that such retention of personal data could help in the fight against crime and terrorism, but subsequently pointed out that interference with an individual's privacy must be minimal and within the limits of applicable EU law.[124]

The European Data Protection Supervisor was satisfied with the ruling and described it as a turning point in the limitations of the government's comprehensive supervision of communications data. Otherwise, there was silence on the part of the institutions. According to Malmström, who was the Commisioner at that time, the ruling and clarification of the right to respect for privacy and data protection had implications for several agreements with the US on passenger registration and the monitoring of terrorist financing. This is a decision that is considered one of the key issues when it comes to privacy and data protection. The collection and use of traffic and location data was controversial even before the directive was adopted. Proposals to repeal the relevant regulations have been initiated before the constitutional courts of several Member States. In others, the European Commission has initiated infringement proceedings. However, the decision was also helped by the constant pressure from civil society against the directive, as well as the evaluation of the directive, which proved unconvincing.[125]

[121] *Digital Rights Ireland…,* para 39.
[122] Ibid., para 64.
[123] GRANGER, M. and K. IRION. The Court of Justice and…, p. 841.
[124] MURPHY, M. "Data retention in the aftermath…, p. 2-6.
[125] GUILD, S. and S. CARRERA. The Political and Judicial Life of Metadata…, p. 9-13.

3.3 Patrick Breyer v Bundesrepublik Deutschland

Mr Breyer brought an action against the Federal Republic of Germany as the operator of a publicly accessible website which provides up-to-date information and stores the IP addresses of visitors. This was because his IP address had been retained due to visits to several German authorities' websites. Such retention is intended to enable criminals to be prosecuted.[126] He based his dismissal on the basis of the Personal Data Protection Act. The Court of First Instance dismissed the action and the Court of Appeal partially amended that decision on the grounds that Germany should not have retained Mr Breyer's IP address after the termination of his internet connection, in the case of IP address retention in connection with the website opening date and of his connection revealing his identity. The Court of Appeal required Germany to refrain from storing a dynamic IP address to the extent that retention is not necessary to restore the internet service in the event of a breakdown. He further stated that in this case, the IP address was considered as personal because Breyer could be identified on its basis. It was decided that in situations where Breyer did not provide his identity during the internet connection, there was no reason to comply with his request. Furthermore, Germany, as an online service provider, does not have an IP address in its possession as personal data, as it cannot identify users of the website in question. As Breyer was not fully satisfied, he appealed against the decision of the Court of Appeal to the German Federal Court of Justice. Germany has done the same with a proposal to reject this.[127]

The German Federal Court referred the case to the CJEU asking whether dynamic IP addresses of website visitors constitute personal data for website operators, and whether a specific data protection provision of the German Telemedia Act, which basically precludes justification based on legitimate interests (Article 7(f) of the Directive), is in line with EU law.[128] The Court asked these questions because it stated that there was a dispute as to whether an objective or relative criterion should be used to determine a person's identifiable nature. As far as the objective criterion is concerned, IP addresses can be perceived as personal data if the data subject can be identified by a third party after the connection to the website has been terminated. Conversely, with the relative criterion we can only talk about personal data as far as the connection provider is concerned because only that provider could identify Breyer.[129]

[126] *Patrick Breyer v Bundesrepublik Deutschland*, C-582/14, Judgment of the Court (Second Chamber), 19 October 2016, para 13-17.
[127] Ibid., para 19-22.
[128] Ibid., para 30.
[129] Ibid., para 25.

The CJEU first referred to the Scarlet Extended decision, which ruled that IP addresses may constitute personal data, but the difference is that in Scarlet Extended IP addresses were collected and subsequently identified by connection providers while Breyer IP addresses were stored by the content provider, although it had no other information needed to identify them.[130] Another issue concerned the difference between dynamic and statistical IP addresses, which represent constant data and allow for the identification of the device. In contrast, a dynamic IP address is assigned on the basis of communication for the so-called lease period. According to the CJEU, a dynamic IP address alone, free from other data, does not in principle reveal the identity of a natural person.[131]

A relative criterion was used in this judgment and the CJEU stated that for a dynamic IP address to be considered personal data, it had to be verified that the dynamic IP address held by the content provider could be qualified as identifiable information. It thus referred to Article 2 of the directive, in conjunction with recital 26 in the preamble to the directive, which provides that it must cover all information relating to an identified or identifiable individual and must take account of all the means which may be used.[132] In the case of Mr Breyer, it is therefore possible that even if another person has information other than the content provider, the IP address will also represent personal data for the provider. An IP address represents personal data in cases where there are legal consequences that allow the data subject to be determined on the basis of other added data. This decision influenced all IP address processors to consider whether they should treat them as personal data. However, the Court has not specified what the legal means of identifying a person are because in practice they will vary from one country to another depending on national legislation and the interpretation of local supervisors.[133]

This decision was a precise response to the constant development of communication technologies, given the scope of what can still be classified as personal data within the meaning of Article 2(a) Directive 95/46/EC. The decision provided a long-term view of dynamic IP addresses, which in conjunction with other data may constitute personal data, which is now set out in the definition of personal data in the GDPR.[134]

---

[130] Ibid., para 33.
[131] Ibid., para 31-39.
[132] Directive 95/46/EC of the European Parliament…, Article 2.
[133] BORGESIUS, F. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data. *heinonline.org* [online]. 2017, 3 Eur. Data Prot. L, [viewed 25 May 2021]. Available from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=23&id=&page=
[134] CJEU decision on dynamic IP addresses touches fundamental DP law questions. *twobirds.com* [online]. 2016 [viewed 16 February 2022]. Available from: https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions

3.4 Tele2 Sverige and Secretary of State for Home Department v Tom Watson

As a result of the Digital Rights Ireland judgment and its declaration of the invalidity of the Data Retention Directive (invalid ex tunc), a harmonized legal framework governing data retention at EU level was unavailable. However, this did not affect the validity of the national provisions of the Member States adopted in this directive. The following joint judgment therefore addresses the implications of Digital Rights Ireland in the legislation of the Member States as well as the compatibility of national data retention measures with the fundamental rights in the CFR.[135]

3.4.1 The facts of the cases

In the case C-203/15, a Swedish provider of electronic communication services Tele2 Sverige informed the Swedish Post and Telecom Authority, the Post-och Telestyrelsen, that with regard to the Digital Rights Ireland judgment, which invalidated Directive 2006/24, it would stop storing electronic communications by 14 April 2014. They stated that they no longer had to do so due to an invalid directive that had become part of national law.[136] The following day the police presidium in Sweden lodged a complaint with PTS against Tele2 Sverige on the grounds that it had ceased to provide them with the information in question.[137] In light of the Digital Rights judgment, an examination of the disputed Swedish legislation was not incompatible with either EU law or the ECHR. As a consequence, the PTS informed Tele2 Sverige that it was in breach of its obligations under LEK (Law on Electronic Communications) and ordered them to start retaining that data. However, Tele2 brought an action against the order before the administrative court, stating that the report was based on a misinterpretation of the Digital Rights judgment.[138]

According to the referring court, the compatibility of Swedish legislation with EU law had to be assessed in accordance with Article 15(1) of Directive 2002/58, concerning the processing of personal data and the protection of privacy in the electronic communications sector. This article provides that

---

[135] TRACOL, X. The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for a harmonised legal framework on the retention of data at EU level. *Computer law & security review* [online]. 2017, vol.33, issue 4 [viewed 16 February 2022], p. 542. Available from: https://www.sciencedirect.com/science/article/pii/S0267364917301607?casa_token=AjFM6KjH43QAAAAA:aeem9Vck4_iv73oxslT7nQdsfTbxfpnvCWQSek2zqhHKMcQv27HbZKyXIyqeTE-ikPoZGfgB4g

[136] *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, C-203/15, Judgment of the Court (Grand Chamber), 21 December 2016, para 44.

[137] Ibid., para 45.

[138] Ibid., para 46-48.

> Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8 (1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (ie State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offenses or of unauthorized use of the electronic communication system….[139]

This article provides for exceptions which limit the obligation to delete or anonymize data, even where this directive lays down the principle of deletion of data as soon as they are no longer necessary for the transmission of the communication.[140] The court asked the CJEU whether it was a general obligation to keep the data of all persons and means of electronic communication without any exceptions or limitations in accordance with the already mentioned Article 15 of the directive with regard to Articles 7, 8 and 52 of the CFR.[141]

In the case C-698/15, Tom Watson and others filed a lawsuit for a judicial review of the lawfulness of the data retention regime in Section 1 of the Data Retention and Investigatory Powers Act of 2014 (DRIPA). According to them, this section was incompatible with articles 7 and 8 of the CFR and Article 8 of the ECHR. The High Court of Justice stated that the regime was in conflict with EU law because it did not satisfy the conditions laid down in the Digital Rights judgment. The court stated that Section 1 DRIPA is not compatible with articles 7 and 8 of the CFR because it does not state how to get access to and use retained data. Later, the Secretary of State for the Home Department brought an action against that judgment before the referring court. The referring national courts requested a preliminary ruling about Article 15 (1) of Directive 2002/58, read in the light of Articles 7, 8 and 52 (1) of the CFR.[142]

The Court of Appeal stayed the proceedings and asked the CJEU two questions. The first dealt with the Digital Rights judgment and, therefore, whether that judgment set out the requirements of EU law which are binding and 'applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Articles 7 and 8 of [the Charter].'[143] The second question concerned the scope of

[139] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Article 15 (1).
[140] *Tele2 Sverige*…, para 49-50.
[141] Ibid., para 51.
[142] Ibid., para 52-58.
[143] Ibid., para 59 (1).

Article 7 or 8 of the CFR, whether the Digital Rights judgment extended the scope of those articles beyond Article 8 of the ECHR.[144]

3.4.2 Joined Judgment

The Court first examined the structure of the directive and distinguished between Article 1(3), which imposes activities outside the scope of the directive, and Article 15(1), which provides for derogations from the law of data subjects.[145] The Court found that Article 15 (1), read in the light of Articles 7, 8 and 52(1) of the CFR, precludes national legislation which provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.[146] The CJEU also found that Article 15(1) must be interpreted as precluding national legislation governing the protection and security of traffic and location data and access of competent national authorities to the retained data, unless it is restricted to solely fighting serious crime, and that it prescribes a requirement of prior review by a court or an independent administrative authority before granting access to the data.[147]

With this judgment the CJEU showed its concern to ensure respect for the CFR, in particular the rights to respect for private life and protection of personal data, which are also set out in Article 8 of the ECHR.[148] The main impact of this judgment was that national legislation which provided for the mass surveillance of electronic communications violated the right to privacy and the right to the protection of personal data, even if the purpose was to combat crime. Directive 2002/58 must be interpreted in favour of Articles 7 and 8 of the CFR and that national authorities are entitled to retain data only for the purpose of combating serious crime, but with prior judicial review. This judgment confirms that general data retention regimes violate fundamental rights and are considered a threat to individuals and their privacy. The judgment first set out EU standards on the retention of personal data for monitoring purposes, which Member States have to comply with. The CJEU has confirmed that it will only accept a strict interpretation of the minimum standards for general data retention and mass surveillance and has limited the possibility for Member States to derogate from the principle of the confidentiality of communications for national security purposes. Therefore, the need has arisen for a harmonized legal framework for data retention at EU level. [149]

[144] Ibid., para 59 (2).
[145] Ibid., para 69-72.
[146] Ibid., para 77.
[147] TRACOL, X. The judgment of the Grand Chamber dated…,p. 545.
[148] Ibid., p. 548.
[149] Ibid., p. 544-549.

4 Austrian citizens and judgments in digital rights matters

This chapter will be dedicated to two Austrian citizens whose initiatives and cases have greatly influenced the protection of digital rights on the internet. However, I would like to begin by briefly outlining the adoption of the GDPR in Austria and a view on the protection of rights in the digital world. The Personal Data Protection Act, which incorporates the GDPR into Austrian law, was adopted in June 2017 with effect from May 2018. Like other countries, Austria set important points for it which are included in the law, such as the application for legal persons, setting the age of 14 for when a child can give valid consent for the processing of their data, and the processing of judgments and crimes by private entities.[150]

In my opinion, it is important to mention the decision of the Austrian Data Protection Authority (DPA) of January this year, which stipulates that the continuous use of Google Analytics by the Austrian website provider and the subsequent transfer of personal data to Google violated the GDPR. This decision resulted from a number of objections raised by the NOYB group dealing with personal data protection, and from the 'Schrems I' and 'Schrems II' judgments, which will be further discussed in this work. Google Analytics is a website traffic monitoring service. Google LLC accepts certain information, such as IP addresses or cookies. Google then evaluates the data and provides statistics to the site operators. The question was whether this data was considered personal data. The DPA ruled that the combination of IP addresses and cookies passed to Google was personal data subject to the GDPR. This is because this data could be combined with other data held by Google to identify individuals.[151] I will now examine the case of Max Schrems, whose initiative was very important for this decision and in several others.

4.1 Max Schrems

Max Schrems is an Austrian lawyer, activist, co-founder of the Europe v Facebook initiative and a very important figure in the field of digital rights protection, as in 2017 he founded the European Centre for Digital Rights NOYB in Vienna. The name stands for 'none of your bussiness', which indicates the main goals of this non-profit organization - privacy issues and privacy violations in the private sector. Under Article 80 of the GDPR, non-profit organizations may act and represent users. Therefore, their main objective is to launch strategic

[150] Datenschutzrecht in Österreich. *gsb.gv.at* [online]. 13 February 2022 [viewed 23 February 2022]. Available from: https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html

[151] BAUMANN, A. DIE ÖSTERREICHISCHE DATENSCHUTZBEHÖRDE SAGT, DIE VERWENDUNG VON GOOGLE ANALYTICS VERSTOSSE GEGEN DIE DSGVO – DATENSCHUT. *presseraum.at* [online]. 13 February 2022 [viewed 23 February 2022]. Available from: https://www.presseraum.at/die-oesterreichische-datenschutzbehoerde-sagt-die-verwendung-von-google-analytics-verstosse-gegen-die-dsgvo-datenschutz/

court cases in support of the GDPR. He became interested in the protection of personal data in connection with Facebook and the fact that he is not able to decipher how Facebook handles his personal data. Another important moment was the revelations concerning the US government's spy programme by Edward Snowden.[152] It transpired that the National Security Agency (NSA) operated surveillance programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of US companies such as Facebook, Microsoft and others.[153]

4.1.1 Schrems v Facebook Ireland Ltd.

Schrems exercised his right to access personal data under the Data Protection Act 1988 and asked Facebook to provide him with all the data they had collected on him. He received a CD with several thousand items of information, much of which had been deleted for a long time. The he filed several complaints against Facebook with the Irish Data Protection Commissioner (DPC), where he challenged, for example, the conditions of data use and the collection of personal data. Some measures were imposed on Facebook, but they were not considered sufficient. Therefore, he brought a class action against Facebook Ltd before the Austrian courts for breaching EU data protection law, which was joined by up to twenty-five thousand people from a number of countries (they passed their claims onto him). The class action imposed an obligation on Facebook to reimburse the plaintiffs for the misuse of personal data.[154]

The Vienna court of first instance declared the class action inadmissible and Schrems was considered an activist rather than a consumer of Facebook because he used Facebook for professional purposes. As a result, he could not rely on the provision regulating consumer contracts. The court also ruled that several users in the class action were not resident in Vienna and some were not even citizens of the EU. The task of the CJEU was to determine the nature of the consumer and to examine whether publishing books or lecturing activities and others meant the loss of the status of a private Facebook user and thus of a consumer.[155] The CJEU stated that the concept of consumer had to be interpreted strictly on the basis of Regulation

[152] KENNEDY, J. The Interview: Max Schrems, privacy activist. *siliconrepublic.com* [online]. 28 January 2015 [viewed 20 February 2022]. Available from: https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video

[153] TZANOU, M. Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights. Data Protection Beyond Borders:Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Publishing, Forthcoming. *papers.ssrn.com* [online]. 12 November 2020 [viewed 20 February 2022], p. 3. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3710539

[154] *Maximilian Schrems v Facebook Ireland Limited*, C-498/16, Judgment of the Third Chamber, 25 January 2018, para 10-15.

[155] Ibid., para 20-24.

44/2001 (jurisdiction in consumer cases) and stated that the above activities did not lead to the loss of consumer status. Schrems, therefore, had the possibility to turn to the EU's rules on jurisdiction in consumer cases and to sue the other party for its consumer contract in its own national courts. The CJEU issued a decision admitting Schrems' individual lawsuit against Facebook in Vienna, but the possibility of a class action lawsuit was ruled out. Although this case dismissed the class action, it is important in the area of freedom of expression and guaranteeing consumer protection.[156]

4.1.2 'Schrems I'

This decision is considered one of the most important in the field of personal data transfer, determining the further development of personal data protection and the overall view of privacy on the internet. Everyone who lives in the EU and wants to use the Facebook application must first enter into an agreement with Facebook Ireland, a subsidiary of Facebook Inc., based in the USA. In 2013, Schrems lodged a complaint with the DPC asking it to ban Facebook Ireland from transferring his personal data to the US due to possible NSA surveillance. However, the application was rejected as unjustified and out of scope, referring to the Commission's Safe Harbour decision and ensuring adequate protection of personal data by the US. Schrems challenged the DPC's decision before the Irish High Court, which decided to refer a question to the CJEU for a preliminary ruling.[157] The first question was whether the authorities were absolutely bound by the Commission's decision when assessing a complaint involving the transfer of personal data to a third country and whose legislation may not provide adequate protection, and whether the office had to carry out its own investigation into the factual situation.[158]

It is important to first outline the legislation that regulates cross-border data flows. Under the Data Protection Act, there are three mechanisms for transferring data to countries outside the EU. The first is a transfer based on a Commission decision stipulating that an adequate level of protection is ensured in a third country.[159] The second mechanism may be implemented on the basis of appropriate safeguards[160] and the third on the basis of certain derogations for a specific situation.[161] A so-called Safe Harbour scheme has been set up between the EU

[156] Maximilian Schrems v. Facebook Ireland Limited. *globalfreedomofexpression.columbia.edu* [online]. [viewed 20 February 2022]. Available from: https://globalfreedomofexpression.columbia.edu/cases/maximilian-schrems-v-facebook-ireland-limited/
[157] TZANOU, M. Schrems I and Schrems II:…, p. 3.
[158] *Maximillian Schrems v Data Protection Commissioner*, C-362/14, Judgment of the Court (Grand Chamber), 6 October 2015, para 36.
[159] GDPR…, Article 45.
[160] Ibid., Article 46.
[161] Ibid., Article 49.

and the US to allow data flow. It was based on the voluntary self-certification of companies which adhere to certain data protection principles. There have also been some interventions by public authorities. On that basis, the Commission issued a decision recognizing the adequate protection afforded by the Safe Harbour Principles. At first, it was seen as a system that improved the level of privacy protection until it was found to be suffering from major deficiencies which were confirmed and deepened by Snowden's revelation.[162]

According to the CJEU, Directive 95/46/EC does not release any national authority from the power to supervise the transfer of personal data to third countries and these authorities are also obliged to assess whether the transfer to third countries meets all the requirements.[163] In that judgment, the CJEU annulled the Commission's decision on the adequate protection of personal data in the Safe Harbour programme. The Court further clarified the criterion of adequate protection by stating that there is no definition of that term.[164] The CJEU stated that the concept of adequate protection can be considered as equivalent rather than the same level of protection as in the EU.[165] In doing so, the Court has made every effort to ensure that national data protection rules are not undermined by the transfer of personal data to third countries. Thanks to this judgment, data protection has been raised to the level of a fundamental right and cross-border data flows should be considered part of the EU institutions' fundamental rights obligations, as individuals cannot be restricted in their rights due to the transfer of their data to third countries. In this case, the essence of the fundamental right to privacy and judicial protection was violated, as US regulations did not provide EU citizens with sufficient legal guarantees and remedies.[166]

This judgment raised questions such as why the CJEU had not examined the infringement on the basis of proportionality, as in Digital Rights Ireland, but was directly inclined to infringe the essence of the right to privacy. However, the CJEU argues that there is no need to discuss violations of the substance of the law when it sees them. As Tzanou said:

> The Court did not come up with a clear methodological approach or a comprehensive doctrinal justification why the essence of this right was breached in that case. It just drew a supposed red line – first laid down in Digital Rights Ireland – between generalised access

[162] TZANOU, M. Schrems I and Schrems II:…, p. 5.
[163] COUDERT, F. Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities. *europeanlawblog.eu* [online]. 15 October 2015 [viewed 20 February 2022], p. 1-2. Available from: https://lirias.kuleuven.be/1711668?limo=0
[164] *Maximillian Schrems v Data Protection Commissioner*…, para 70.
[165] Ibid., para 73.
[166] TZANOU, M. Schrems I and Schrems II:…, p. 6.

to the content of communications and access to metadata, and concluded that the former constitutes the essence of the fundamental right to privacy.[167]

The 15-year Commission decision on the EU-US data flow agreement was therefore overturned by the ruling, and the CJEU ruled that even if US companies took adequate privacy and data protection measures, US authorities would still not be subject to the agreement and therefore the privacy of EU citizens has been threatened by government oversight again.[168] The CJEU has decided that third countries must in the future ensure 'by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order.'[169]

4.1.3 'Schrems II'

Following the repeal of the decision on the validity of the Safe Harbour, the Privacy Shield was adopted in 2016. It was also based on a system of certification by US organizations and their commitment to privacy. This regime was based on a decision of the Commission which reflected the commitments and declarations of the US government. Companies that process EU user data were required to make the data available to US security services, and the Privacy Shield was intended to ensure a standard of protection with the EU. However, concerns have been raised about the lack of oversight of US surveillance programmes and whether the decision complies with EU privacy and data protection standards.[170] The Privacy Shield and its analysis was based solely on a description of US law, without the US authorities making the substantial commitments required by the EU. After the invalidation of Safe Harbour, Schrems turned to the DPC again and asked it to suspend the transfer of his data to Facebook Inc. so that the data could not be accessed by the NSA or the FBI. The DPC brought proceedings before the Irish High Court, which submitted a reference to the CJEU for a preliminary ruling.

In that judgment, the CJEU annulled the Privacy Shield decision and set a standard of protection according to which the Commission should assess decisions on adequacy 'with the requirements stemming from the GDPR read in the light of the Charter'.[171] It thus ruled that

---

[167] Ibid., p. 9.
[168] LOIDEAN, N. The End of Safe Harbour: Implications for EU Digital Privacy and Data Protection Law. *Journal of Internet Law* [online]. 21 February 2016, Vol. 19, Issue 8 [viewed 21 February 2022], p. 10. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2734698
[169] *Maximillian Schrems v Data Protection Commissioner*…, para 96.
[170] TRACOL, X. "Schrems II": The return of the Privacy Shield. *Computer Law and Security review* [online]. 2020 [viewed 21 February 2022], p. 3. Available from: https://www.sciencedirect.com/science/article/pii/S0267364920300893?casa_token=3KEOGgGfrwgAAAAA:TN4GbdT6wsWtBCNqB4lev1j64DFz98nWsnhEXz2P0_l3MsPVHQr83M1Y4S2s3PzAwSO1G_NV0w
[171] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18, Judgment of the Grand Chamber, 16 July 2020, para 161.

the requirements of US national law and the programmes that allow access to personal data by US authorities for national security purposes do not meet the requirements required by EU law. This judgment also examined the validity of standard contractual clauses. Therefore, the transfer of personal data cannot take place within the Privacy Shield but on the basis of the regime of standard contractual clauses, the validity of which was confirmed. The CJEU considers them to be effective mechanisms enabling the level of protection guaranteed in the EU if companies have verified that the required level of data protection is guaranteed in a particular third country.[172] The 'Schrems I' and 'Schrems II' decisions have contributed to the need for giants such as Google or Facebook to use GDPR as appropriate protection by repealing two Commission adequacy decisions.[173]

4.2 Eva Glawischnig-Piesczek

The Austrian politician Eva Glawischnig-Piesczek sued Facebook Ireland over a request to remove a comment posted by a user on Facebook, which damaged her reputation. This user shared an article by an Austrian magazine on his personal profile, which also included a photograph of Mrs Glawischnig-Piesczek, who was the chair of the Green Party and a member of the National Council. While sharing this post, the user added a comment to Mrs Glawischnig-Piesczek, which was offensive. This post was accessible to any Facebook user.[174]

Glawischnig-Piesczek sent a letter to Facebook Ireland requesting the removal of this offensive comment. According to the plaintiff, there was a violation of Section 78 of the Austrian copyright law - the right to the protection of her image.[175] As her request was not granted, she applied to the Commercial Court in Vienna. The court ordered the company to refrain from disclosing information or sharing photographs of the applicant immediately. At that instigation, Facebook Ireland denied all users access to a specific contribution, but appealed to the Vienna Higher Regional Court. The court upheld the order given at first instance. However, it decided that it was necessary to refrain from disseminating only those allegations which Facebook Ireland had learned from the applicant in the main proceedings or from third

[172] TRACOL, X. "Schrems II": The return of the Privacy Shield…, p. 4-5.
[173] ATIK, J. and X. GROUSSOT. A Weaponized Court of Justice in Schrems II. *Nordic Journal of European Law Law* [online]. 2021, Vol. 4, No. 2 [viewed 21 February 2022], p. 2. Available from: https://journals.lub.lu.se/njel/issue/view/3289
[174] *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, C-18/18, Judgment of the Court (Third Chamber), 3 October 2019, para 10-12.
[175] NOTI, K. Injunctions and Article 15(1) of the E-Commerce Directive: The Pending Glawischnig-Piesczek v. Facebook Ireland Limited Preliminary Ruling. *Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments* [online]. 2018, 5/2018 [viewed. 29 May 2021]. p. 4. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3291599

parties.[176] Both courts justified their decision by reference to Section 78 of the Copyright Act and Section 1330 of the Civil Code, according to which the commentary disproportionately harms the plaintiff, and these insults were not based on demonstrable evidence. An appeal has been lodged with the Supreme Court as to whether an injunction may be imposed on a hosting provider operating a social network with a large number of users, including statements having the same wording or equivalent content but with which the provider was unfamiliar.[177]

In particular, the Austrian Supreme Court requested from the CJEU a clarification of the scope of Article 15 (1) the e-commerce directive. The Court had to clarify whether an injunction could order a provider's control obligation to remove not only the reported illegal circulation but also identically worded information.[178] If the answer were in the affirmative, the Court asked whether this would also apply to content of equivalent importance and whether this effect could be felt worldwide.[179] This directive stipulates that the host platform is not obliged to be liable for content created by the users themselves, unless they themselves have knowledge of the illegality of that content. This only prohibits monitoring obligations of a general nature.[180]

Article 15 serves to promote the fundamental freedoms protected by both the CFR and the ECHR.[181] In this case, the Court referred to Article 14 (1) of the directive, which exempts information service providers from liability. However, this is the case if they do not know about the illegal activity or if they act as soon as they find out about it. In these cases, it is possible to request the removal of illegal content and prevent further violations. Although Article 15 (1) prohibits general monitoring of online content, it allows monitoring in specific cases where content has been declared illegal.[182]

In this case, the company knew about the illegal content and did not act to remove it.[183] The CJEU has ruled that the directive does not preclude ordering online content providers to remove illegal information as well as identical or equivalent information. This monitoring falls

[176] *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, C-18/18, Judgment of the Court (Third Chamber), 3 October 2019, para 13-16.
[177] Ibid., para 17-19.
[178] NOTI, K. Injunctions and Article 15(1)…, p. 8.
[179] *Eva Glawischnig-Piesczek v Facebook…*, para 20 (2).
[180] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Article 14-15.
[181] Charter of Fundamental Rights…., Article 10.
[182] BROGI, E. and M. MARONI. Eva Glawischnig-Piesczek V Facebook Ireland Limited: a new layer of neutrality. *cmpf.eui.eu* [online]. 17 October 2019 [viewed 23 February 2022]. Available from: https://cmpf.eui.eu/eva-glawischnig-piesczek-v-facebook-ireland-limited-a-new-layer-of-neutrality/
[183] *Eva Glawischnig-Piesczek v Facebook Ireland Limited*…, para 31.

under the permitted control in the specific case and there is, therefore, no breach of the general prohibition on monitoring. The equivalent information in this case means information with essentially the same meaning but different wording.[184] As far as geographical scope is concerned, the CJEU has determined that it is the responsibility of the Member State to determine the scope of these restrictions, but this must be within the framework of the relevant international law. It thus referred to Article 18 (1), which does not lay down any provision limiting the effects of those injunctions. It is therefore possible for Member States to order the removal of illegal content worldwide. This decision has raised concerns about freedom of expression. In connection with the judgment, the understanding of the ban on general monitoring obligations of hosting providers was reconsidered. An intermediary covered by a liability waiver should be considered a hosting provider. The platform should not have knowledge of the content distributed through its service, but if information about illegal activity arises, it must remove this information.[185]

[184] Ibid., para 41.
[185] BROGI, E. and M. MARONI. Eva Glawischnig-Piesczek…

Conclusion

In this Master's thesis, I dealt with the issue of Digital Fundamental Rights in the case law of the CJEU as it concerns digitalization - an area that is constantly evolving and is increasingly interfering with the everyday lives of all people. Modern technology and how people use the internet can violate people's privacy and, in this case, result in a breach of personal data protection, which should be well guarded. We are also living in a different era in which we are willing to provide a large amount of information about ourselves. This information becomes publicly available to everyone. The problem also occurs with "forgetting" on the internet. What we share somewhere on different sites and on social networks may not simply go back. That's why it is important to constantly respond to these changes and to protect the rights of data subjects. Precisely because of the rapid development of technology, states are unable to adopt legislation and other regulations immediately. The preparation and adoption of such regulations takes a very long time and is preceded by a great deal of debate.

In the first part of this work, I focused on digital fundamental rights, their outline and the specific rights within the CFR and GDPR. An important point was to introduce the RTBF, which, thanks to the case law of the CJEU, has become a very important right on the internet. Thanks to the RTBF and the deletion of personal data, a balance can be struck between an individual's privacy and the processing of their data. The next part of my work was devoted to the judgments themselves, which in my opinion and the opinion of experts have had the biggest influence on functioning of the digital sphere and the protection of human rights. I analysed the individual cases, their origin, circumstances and, of course, the impacts that emerged from the judgments. Based on the descriptive method and analysis, I tried to answer questions about the CJEU case law, their impacts, effectiveness and the RTBF itself and its effectiveness.

In my opinion, the hypothesis: *'The CJEU case law responds effectively to the pace of development of the digital world, thus ensuring reliable protection of individuals' digital rights.'* was confirmed as there is a relatively large body of case law on this subject and protection has been affected in many areas. The case law of the CJEU is extremely important because it is the Court's decision in specific cases which can respond to the evolving situation and thus affect the provision of fundamental rights in the digital world. The CJEU case law has played an important role, for example, in the formation of the GDPR regulation, which contains the RTBF. The specific situation and then the preliminary questions referred to the CJEU have helped to ensure more effective protection of human rights on the internet and to

adjust the various rules for internet search engines or personal data processors. In some cases, a Court decision is the first step towards new legislation. From my point of view, the CJEU responds effectively to the development of digitization and thus ensures better protection of the rights of individuals. In most cases, it is only specific situations that reveal errors or human rights violations and the CJEU can respond as best it can to these situations. Of course, the decisions also have consequences that can affect both individuals and search engines or processors of personal data. In any event, the Court has made every effort to protect the rights of individuals and to ensure that search engines or processors of personal data operate in a way that does not infringe rights. However, each case was unique, when the method of proportionality or certain restrictions had to be used on both sides. In these cases, there is a constant conflict of fundamental rights, such as the right to privacy, the protection of personal data, the right to freedom of expression and the right to information. The Court therefore had to clearly define which right should prevail and under what circumstances.

The second hypothesis sets that: *'The RTBF is an adequate legal instrument for personal data protection.'* The RTBF is undoubtedly a very good and effective tool, but it is not possible to rely on it in all cases. We can consider this right as the first major instrument that allows individuals to protect their privacy on the internet. As this quite a 'new right', there are, of course, several problems and unresolved issues, which will, however, be resolved on the basis of further developments and case law of the CJEU. It should primarily be up to people to protect their privacy and sensitive data and not share all their information about themselves. However, it is an effective tool that gives us at least basic control over our data and take advantage of the possibility of forgetting on the internet. It is necessary to keep the general public aware of this right so that they know that they have such an opportunity. As the RTBF is only recognized within the EU Member States, it is, in my view, necessary to secure an agreement between the EU and the US in order to further strengthen this protection.

When writing this thesis, I drew from articles by various experts, book resources, and particularly from EU legislation and international treaties. Many authors from different Member States respond to the case law and shed more light on the implications for personal data protection but also for the impact of decisions on non-EU countries or other related issues. An especially important source was the case law itself which is published on the official website of the CJEU. As this is a relatively 'new' topic, which is under much discussion today and constantly changing with new knowledge, I tried to cover the issue and draw from the views of experts and significant individuals.

Resources

Literature

BRÄUTIGAM, T. and S. MIETTINEN. *Data protection, Privacy and European Regulation in the Digital age*. Helsinki: Unigrafia, 2016. ISBN 978-951-51-2530-9.

Handbook on European data protection law. Luxembourg: Publications Office of the European Union, 2018. ISBN 978-92-9491-903-8.

JONES, M. *Ctrl + Z: the right to be forgotten*. New York: New York University Press, 2016. ISBN 978-1-4798-8170-3.

LAMBERT, P. *Understanding the new European data protection rules*. Boca Raton: CRC Press, Taylor & Francis Group, an Auerbach book, 2020. ISBN 9781138069831.

MENDEL, T. and others. *Global survey on internet privacy and freedom of expression*. Paris: the United Nations Educational, Scientific and Cultural Organization, 2012. ISBN 978-92-3-104241-6.

RHOEN, M. *Big Data, Big Risks, Big Power Shifts: Evaluating the GDPR as an instrument of risk control and power redistribution in the context of big data.* Universiteit Leiden, 2019. ISBN 978-94-6375-465-1.

TZANOU, M. *Personal data protection and legal developments in the European Union*. Hershey, PA: Information Science Reference, 2020. ISBN 9781522594895.

WERRO, F. Balancing the Freedom of Expression Against the General Right to Privacy: The European Approach vs. the United State's Approach. In: Franz Werro (ed.). *The Right to be Forgotten: A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas and Asia*. Cham: Springer, 2020. ISBN 978-3-030-33514-4.

Internet resources

Articles in online periodicals

ATIK, J. and X. GROSSOUT. A Weaponized Court of Justice in Schrems II. *Nordic Journal of European Law Law* [online]. 2021, Vol. 4, No. 2 [viewed 21 February 2022]. Available from: https://journals.lub.lu.se/njel/issue/view/3289

AUSLOOS, J. The 'Right to be Forgotten' – Worth remembering? *Computer Law & Security Review* [online]. 2012 [viewed 10 February 2021]. Available from: https://is.muni.cz/el/law/jaro2019/SOC022/um/59943709/The__Right_to_be_Forgotten__-_Worth_remembering.pdf

BENNET, S. The "Right to Be Forgotten": Reconciling EU and US Perspectives. *Berkeley Journal of International Law* [online]. 2012 [viewed 2 February 2022]. Available from: https://lawcat.berkeley.edu/record/1125027

BORGESIUS, F. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data. *heinonline.org* [online]. 2017, 3 Eur. Data Prot. L [viewed. 25 May 2021]. Available from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=23&id=&page=

BOWDEN, D. CJEU rules director of failed company has no right to be forgotten at Companies House. *ewriter.eu.* [online]. 9 March 2017 [viewed 15 April 2021]. Available from: http://www.ewriter.eu/articles/Manni.pdf

BROGI, E. and M. MARONI. Eva Glawischnig-Piesczek V Facebook Ireland Limited: a new layer of neutrality. *cmpf.eui.eu* [online]. 17 October 2019 [viewed 23 February 2022]. Available from: https://cmpf.eui.eu/eva-glawischnig-piesczek-v-facebook-ireland-limited-a-new-layer-of-neutrality/

BUNN, A. The Curious Case of the Right to Be Forgotten. *Computer Law & Security Review* [online]. 2015, no. 3 [viewed 20 April 2021]. Available from: https://www.sciencedirect.com/science/article/pii/S026736 4915000606

CARAVA, E. Personal Data Kept in Companies Registers: The Denial of the Right to Be Forgotten. *Eur. Data Prot. L. Rev.* [online]. 2017 [viewed 11 February 2022]. Available from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl3&div=52&id=&page=

COUDERT, F. Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities. *europeanlawblog.eu* [online]. 15 October 2015 [viewed 20 February 2022]. Available from: https://lirias.kuleuven.be/1711668?limo=0

GLOBOCNIK, J. The Right to Be Forgotten is Taking Shape: CJEU Judgments in *GC and Others* (C-136/17) and *Google v CNIL* (C-507/17). *GRUR International* [online]. 2020, vol.69, issue 4 [viewed 15 April 2021]. Available from: https://academic.oup.com/grurint/article/69/4/380/5732807

GODDARD, M. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research* [online]. 2017, Vol. 59, Issue 6 [viewed 28 January 2022]. Available from: https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050?journalCode=mrea

GRANGER, M. and K. IRION. The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection. *European Law review* [online]. 2014 [viewed 15 February 2022]. Available from: https://pure.uva.nl/ws/files/65990842/The_Court_of_Justice_and_The_Data_Retention_Directive_in_Digital_Rights_Ireland_Kristina_Irion_and_Marie_Pierre_Granger.pdf

GSCHNELL, M. and M. WEIDEMAN. A critical study of "The Right to be forgotten" – a Google case Study. *Working paper* [online]. Munich University of Applied Science, Munich, 2014 [viewed 9 January 2022]. Available from: https://www.researchgate.net/publication/324542829_A_critical_study_of_The_right_to_be_forgotten_-_a_Google_case_Study_0154

GUADAMUZ, A. Developing a Right to be Forgotten [online]. *University of Sussex* [online]. 2017 [viewed 4 February 2021]. Available from: https://www.researchgate.net/publication/320985071_Developing_a_Right_to_be_Forgotten

GUILD, S. and S. CARRERA. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive Elspeth Guild and Sergio Carrera. *Paper in Liberty and Security in Europe* [online]. 2014 [viewed 15 February 2022]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901

HAMULAK, O. and H. KOCHARYAN. The Global Reach of the Right to be Forgotten through the Lenses of the Court of Justice of the European Union. *Researchgate.net* [online]. 2021 [viewed 10 March 2022]. Available from: https://www.researchgate.net/publication/357430418_The_Global_Reach_of_the_Right_to_be_Forgotten_through_the_Lenses_of_the_Court_of_Justice_of_the_European_Union

IGLEZAKIS, I. The Right to Be Forgotten in the Google Spain Case (case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet? *Paper presented at the 4th International Conference on Information Law* [online]. 27 July 2014 [viewed 9 February 2022]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472323

JONES, M. It's About Time: Privacy, Information Lifecycles, and the Right to Be Forgotten *Stanford Technology Law Review* [online]. 2013, vol. 16, no. 2 [viewed 10 February 2021]. Available from: http://ssrn.com/abstract=2154374

KAMPARK, B. To Find or be Forgotten: Global Tensions on the Right to Erasure and Internet Governance. *Journal of Global Faultlines* [online]. 2015, 2(2) [viewed 2 February 2022]. Available from: https://www.jstor.org/stable/10.13169/jglobfaul.2.2.0001#metadata_info_tab_contents

KEYDER, V. Introductory note to the European Court of Justice: Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs, ed editeurs SCRL (SABAM). *International Legal Materials* [online]. 2012, vol. 51 [viewed 11 May 2021]. Available from: https://www.jstor.org/stable/10.5305/intelegamate.51.2.0382?casa_token=sGecAvFaIKsAAAAA%3A2Yvi7Ph1IrnPGwQILlmc7m71pG0nAO3PgjHftSTn-LOBKIBE-wOovfn-DQON-axaqs5az1lEpPaTEomQdYFkTgL-unIVuF4OgTHQyE7NrdtELBHGkD4&seq=1#metadata_info_tab_contents

KULK, S. and F. BORGESIUS. Privacy, freedom of expression, and the right to be forgotten in Europe. In: Jules Polonetsky, Omer Tene, Evan Selinger (eds.) *Cambridge Handbook of Consumer Privacy* [online]. 2018. Available from: https://www.researchgate.net/publication/320456033_Privacy_freedom_of_expression_and_the_right_to_be_forgotten_in_Europe

LOIDEAN, N. The End of Safe Harbour: Implications for EU Digital Privacy and Data Protection Law. *Journal of Internet Law* [online]. 21 February 2016, Vol. 19, Issue 8 [viewed 21 February 2022]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2734698

MURPHY, M. "Data retention in the aftermath of Digital Rights Ireland and Seitlinger." *researchgate.net* [online]. 2014 [viewed 15 February 2022]. Available from: https://www.researchgate.net/publication/291787781_"Data_retention_in_the_aftermath_of_Digital_Rights_Ireland_and_Seitlinger"

NEVILLE, A. Is it a Human Right to be Forgotten? Conceptualizing the World View. *Santa Clara Journal of International Law* [online]. 2017, 15(2) [viewed 2 February 2022]. Available from: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1221&context=scujil

NOTI, K. Injunctions and Article 15(1) of the E-Commerce Directive: The Pending Glawischnig-Piesczek v. Facebook Ireland Limited Preliminary Ruling. *Stanford - Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments* [online]. 2018, 5/2018 [viewed 29 May 2021]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3291599.

POLITOU, E. et al. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* [online]. 2018, 20(1) [viewed 3 January 2022]. Available from: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056?login=true

POST, R. Data privacy and dignitary privacy: Google Spain, the Right to be forgotten, and the construction of the public sphere. *Duke Law Journal* [online]. 2018 [viewed 15 January 2021]. Available from: https://core.ac.uk/download/pdf/213019831.pdf

RAZMETAEVA, Y. The Right to Be Forgotten in the European Perspective. *TalTech Journal of European Studies* [online]. 2020, Vol. 10, No.1 [viewed 10 March 2022]. Available from: https://sciendo.com/article/10.1515/bjes-2020-0004

RUSTAD, M. and KULEVSKA, S. Reconceptualizing the Right to be Forgotten to enable Transatlantic Data Flow. *Harvard Journal of Law & Technology* [online]. 2015, 28(2) [viewed 2 February 2022]. Available from: http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech349.pdf

STAINFORTH, E. Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union. *Journals.sagepub* [online]. 2021 [viewed 2 February 2022]. Available from: https://journals.sagepub.com/doi/pdf/10.1177/17506980211044707

TRACOL, X. "Schrems II": The return of the Privacy Shield. *Computer Law and Security review* [online]. 2020 [viewed 21 February 2022]. Available from: https://www.sciencedirect.com/science/article/pii/S0267364920300893?casa_token=3KEOGgGfrwgAAAAA:TN4GbdT6wsWtBCNqB4lev1j64DFz98nWsnhEXz2P0_l3MsPVHQr83M1Y4S2s3PzAwSO1G_NV0w

TRACOL, X. The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: The need for a harmonised legal framework on the retention of data at EU level. *Computer law & security review* [online]. 2017, vol.33, issue 4 [viewed 16 February 2022]. Available from: https://www.sciencedirect.com/science/article/pii/S0267364917301607?casa_token=AjFM6KjH43QAAAAA:aeem9Vck4_iv73oxslT7nQdsfTbxfpnvCWQSek2zqhHKMcQv27HbZKyXIyqeTE-ikPoZGfgB4g

TZANOU, M. Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights. Data Protection Beyond Borders:Transatlantic Perspectives on Extraterritoriality and Sovereignty, Hart Publishing, Forthcoming. *papers.ssrn.com* [online]. 12 November 2020 [viewed 20 February 2022]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3710539

Contributions within websites

BAUMANN, A. DIE ÖSTERREICHISCHE DATENSCHUTZBEHÖRDE SAGT, DIE VERWENDUNG VON GOOGLE ANALYTICS VERSTOSSE GEGEN DIE DSGVO – DATENSCHUT. *presseraum.at* [online]. 13 February 2022 [viewed 23 February 2022]. Available from: https://www.presseraum.at/die-oesterreichische-datenschutzbehoerde-sagt-die-verwendung-von-google-analytics-verstosse-gegen-die-dsgvo-datenschutz/

BLANKERTZ, A and J. JAURSCH. How the EU plans to rewrite the rules for the internet. *brookings.edu* [online]. 21 October 2020 [viewed 15 January 2021]. Available from: https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-the-internet

CJEU decision on dynamic IP addresses touches fundamental DP law questions. *twobirds.com* [online]. 2016 [viewed 16 February 2022]. Available from: https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions

CNIL orders Google to apply delisting on all domain names of these archengine. *cnil.fr* [online]. 12 June 2015 [viewed 8 May 2021]. Available from: https://www.cnil.fr/fr/node/15790

Datenschutzrecht in Österreich. *gsb.gv.at* [online]. 13 February 2022 [viewed 23 February 2022]. Available from: https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html

EU Court decides on two major "right to be forgotten" cases: there are no winners here. *accessnow.org* [online]. 23 October 2019 [viewed 6 April 2021]. Available from: https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/

EU Data Protection Directive. *uk.practicallaw.thomsonreuters.com* [online]. 1 January 2019 [viewed 10 April 2021]. Available from: https://uk.practicallaw.thomsonreuters.com/6-501-7455?transitionType=Default&contextData=(sc.Default)&firstPage=true

European Parliament adopts draft of Digital Services Act. *openaccessgovernment.org* [online]. 21 January 2022 [viewed 27 January 2022]. Available from: https://www.openaccessgovernment.org/digital-services-act-2/128056/

FLEISCHER, P. Adapting our approach to the European right to beforgotten. *blog.google.com* [online]. 4 March 2016, [viewed 8 May 2021]. Available from: https://www.blog.google/around-the-globe/google-europe/adapting-our-approach-to-european-rig/

GDPR: Right of Access. *gdpr-info.eu* [online]. [viewed 12 February 2021]. Available from: https://gdpr-info.eu/issues/right-of-access/

How should one person's right to be forgotten be balanced with the public's right to information? *archive.google.com* [online]. [viewed 20 April 2021]. Available from: https://archive.google.com/advisorycouncil/

KENNEDY, J. The Interview: Max Schrems, privacy activist. *siliconrepublic.com* [online]. 28 January 2015 [viewed 20 February 2022]. Available from: https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video

LINDSAY, D. The "right to be forgotten" is not censorship. *monash.edu* [online]. 2012 [viewed 3 February 2022]. Available from: https://www.monash.edu/news/opinions/the-right-to-be-forgotten-is-not-censorship

LYNSKEY, O. Rising like a Phoenix: The 'Right to be Forgotten' before the ECJ. *europeanlawblog.eu* [online]. 13 May 2014 [viewed 19 February 2022]. Available from: https://europeanlawblog.eu/2014/05/13/rising-like-a-phoenix-the-right-to-be-forgotten-before-the-ecj/

MACH, Martin. Právo být zapomenut jako reakce na vývoj informačních technologií. *Právník* [online]. 2021 [viewed 8 February 2022]. Available from: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2021/7/7_Mach_597-609_7_2021.pdf

Maximilian Schrems v. Facebook Ireland Limited. *globalfreedomofexpression.columbia.edu* [online]. [viewed 20 February 2022]. Available from: https://globalfreedomofexpression.columbia.edu/cases/maximilian-schrems-v-facebook-ireland-limited/

MCGOWAN, I. The Digital Services Act could make or break European democracy. *euractiv.com* [online]. 25 November 2020 [viewed 7 February 2021]. Available from: https://www.euractiv.com/section/digital/opinion/the-digital-services-act-could-make-or-break-european-democracy/

My Privacy is None of Your Business. *noyb.eu* [online]. [viewed. 27 May 2021]. Available from: https://noyb.eu/en

NADEGE, M. and N. SHABESTARI. The right to be forgotten: the CJEU sides with Google in two landmark cases. *Dataprotectionreport.com* [online]. 9 October 2019 [viewed 8 May 2021]. Available from: https://www.dataprotectionreport.com/2019/10/the-right-to-be-forgotten-the-cjeu-sides-with-google-in-two-landmark-cases/

Personal Information Removal Request Form. *google.com* [online]. [viewed 20 April 2021]. Available from: https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&hl=en

"PRISM 2.0" – Complaints after the Judgment C-362/14. *europe-v-facebook.org,* [online]. [viewed 29 May 2021]. Available from: http://www.europe-v-facebook.org/EN/Complaints/PRISM_2_0/prism_2_0.html

SAMONTE, M. Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law. *europeanlawblog.eu.* [online]. 29 October 2019 [viewed 11 May 2021]. Available from: https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law

Scarlet Extended SA v. SABAM. *globalfreedomofexpression.columbia.edu* [online]. [viewed 15 February 2022]. Available from: https://globalfreedomofexpression.columbia.edu/cases/scarlet-extended-sa-v-sabam/

The Advisory Council to Google on the Right to be Forgotten. *static.googleusercontent.com* [online]. 6 February 2015 [viewed 9 February 2022]. Available from: https://static.googleusercontent.com/media/archive.google.com/cs//advisorycouncil/advisement/advisory-report.pdf

The GDPR for EU institutions: your rights in the digital era. *eda.europa.e*u [online]. [viewed 10 February 2021]. Available from: https://www.eda.europa.eu/docs/default-source/documents/your-rights-in-digital-era---factsheet-1.pdf

The INTERNET is a public good. *waccglobal.org* [online]. 27 August 2017 [viewed 15 January 2021]. Available from: https://waccglobal.org/the-internet-is-a-public-good/#:~:text=ARTICLE%2019%20believes%20that%20the,be%20both%20necessary%20and%20proportionate

The right to be informed (transparency) (Article 13 & 14 GDPR). *dataprotection.ie* [online]. [viewed 10 February 2021]. Available from: https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-14-gdpr#:~:text=The%20principle%20of%20transparency%20requires,and%20plain%20language%20be%20used.

ZSIROS, S. What is the EU Digital Services Act and how will it impact Big Tech? *Euronews.com* [online]. 20 January 2022 [viewed 27 January 2022]. Available from: https://www.euronews.com/2022/01/20/what-is-the-eu-digital-services-act-and-how-will-it-impact-big-tech

Cases

Amann v. Switzerland, ECtHR, Application No. 27798/95, Judgment, 16 February 2000.

Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, C-398/15, Judgment of the Court (Second Chamber), 9 March 2017.

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18, Judgment of the Grand Chamber, 16 July 2020.

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, C-293/12, Judgment of the Court (Grand Chamber), 8 April 2014.

GC and Others v Commission nationale de l'informatique et des libertés (CNIL), C-136/17, Judgment of the Court (Grand Chamber), 24 September 2019.

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, Judgment of the Court (Grand Chamber), 13 May 2014.

Leander v. Sweden, ECtHR Application No. 9248/81, Judgement, 26 March 1987.

Maximillian Schrems v Data Protection Commissioner, C-362/14, Judgment of the Court (Grand Chamber), 6 October 2015.

Maximilian Schrems v Facebook Ireland Limited, C-498/16, Judgment of the Third Chamber, 25 January 2018.

Mosley v. the United Kingdom, ECtHR, Application No. 48009/08, Judgement, 10 May 2011.

Opinion of Advocate General delivered on 25 June 2013 (1), Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González

Opinion of Advocate General Szpunar delivered on 10 January 2019 (1), Case C-136/17.

Patrick Breyer v Bundesrepublik Deutschland, C-582/14, Judgment of the Court (Second Chamber), 19 October 2016.

Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, Judgment of the Court (Third Chamber), 24 November 2011.

Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, C-203/15, Judgment of the Court (Grand Chamber), 21 December 2016.

Legislation

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Regulation (EU) No 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.

International Treaties and Other Documents

Charter of Fundamental Rights of the European Union (2012/C 326/02), 2000, Nice.

Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, 1950, Rome.

Treaty on the Functioning of the European Union, Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, 13 December 2007.

Abstract

This Master's thesis deals with the analysis of Digital Fundamental Rights in the case law of the CJEU. As technology is constantly evolving and digitization is increasing, it is necessary to address this issue in the protection of fundamental human rights on the internet. People share a lot of information about themselves and their lives that can be misused by both personal data processors and internet search engines. Therefore, in some cases, serious harm can be prevented if there is also a secure space on the internet that ensures at least basic human rights protection. This thesis outline the issue of Digital Fundamental Rights and freedoms of individuals in the EU with an emphasis on the GDPR and the Right to be forgotten. The main aim is to analyse the rulings of the CJEU in this area, i.e. case law focusing on the right to be forgotten, data protection, privacy on internet networks and content regulation and to find out the impact of the decisions on the protection of fundamental rights.

Key words

Digital Fundamental Rights – GDPR – Privacy – Protection of Personal data – Right to be forgotten – The Court of Justice of the European Union

Abstrakt

Tato diplomová práce se zabývá analýzou základních digitálních práv v judikatuře SDEU. Vzhledem k tomu, že technologie se neustále vyvíjí a process digitalizace se dostává na stale vyšší úroveň, je nutné se touto problematikou zabývat i v rámci ochrany základních lidských práv na internetu. Lidé o sobě a svém životě sdílejí mnoho informací, které mohou být zneužity jak zpracovateli osobních údajů, tak internetovými vyhledávači. Proto lze v některých případech předejít vážné újmě, pokud na internetu existuje také bezpečný prostor, který zajišťuje alespoň základní ochranu lidských práv. Tato práce nastiňuje problematiku digitálních základních práv a svobod jednotlivců v EU s důrazem na GDPR a Právo být zapomenut. Hlavním cílem je analyzovat judikaturu SDEU v této oblasti, tj. judikaturu zaměřenou na právo být zapomenut, ochranu údajů, soukromí na internetových sítích a regulaci obsahu a zjistit dopady těchto rozhodnutí na ochranu základních práv.

Klíčová slova

Základní digitální práva – GDPR – Soukromí – Ochrana osobních údajů – Právo být zapomenut – Soudní dvůr Evropské unie