General Data Protection Regulation: The right to erasure

Sofia Bika

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation

January 2020

Thessaloniki – Greece

Student Name: Sofia Bika

SID: 1104170004

Supervisor: Prof. Komninos Komnios

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

January 2020

Thessaloniki - Greece

Abstract

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation at the International Hellenic University.

The protection of personal data is at the heart of the interest and plays great role both socially and economically. The adoption of General Data Protection Regulation by the European Union created the right conditions for a better interpretation of the concept of personal data and for its practical implementation. It set out the new framework for protecting the personal data of European Union citizens in general and in particular the rules on their collection, use and storage, while enacting the right to erasure which is one of the most debated and controversial rights in the digital age.

This study will first examine the concept and nature of personal data and data protection, the concepts and scope of the right to erasure and the relation between the right to erasure and other fundamental rights and freedoms, such as the freedom of expression, the right to historical memory, the freedom to conduct a business and the right to intellectual property. It will follow a reference to the 'time' as a determinative factor about erasure or retention of data and, finally, a reference will be made to the technological challenges in applying the right to erasure.

Finally, I would like to thank my Supervisor, Prof. Komninos Komnios, for his guidance and support in writing this Thesis.

Keywords: right to be forgotten, right to erasure, GDPR, digital memory

Sofia Bika

10-01-2020

Contents

1. INTRODUCTION

The rapid evolution of the Internet and its participatory nature have led to increased risks to the right to privacy, in particular in view of the technological possibilities provided for electronic user monitoring. Especially, due to the rapid technological advancement, a large amount of personal information is collected daily for each of us. These information include, among others, where we have moved, what our preferences are, what searches we have made on the internet, what recordings are available on the Internet regarding our family, our work, our public image. Thus, intentionally or not, our online profile is created, and the accumulation of large amounts of data is attained. Although the data is collected by a large number of public and private organizations and not by one, a really important question, especially today, is the role of search engines. It should also be noted that the storage of information is not only done by large organizations such as search engines, social media and application providers, but users themselves in the current form of the Internet, play an important role in the processing and sharing of data, re-produce data for themselves as well as for others.

As everybody knows, information posted on the web is never forgotten. The problem becomes more obvious when information published on the internet no longer corresponds to the individual's image, especially when they are revealed without his consent, when they are inaccurate, misleading, or even worse completely false, or when the damage caused by the disclosure is not remedied.

There is one thing that we can say for sure: our society is an information-hungry society. Everybody asks for more and more information: advertising companies, public sector, individuals. There is a constantly ability to record each and every interaction of an individual’s life. Every activity which is mediated by a computer generates personal data that can be captured by anyone who wishes to use them to serve their purposes, regardless of the subject's will. Both our on-line behavior and our off-line behavior can easily be monitored.

It is an undisputed fact that search engines can collect a large number of data through web browsing or even mouse-moving[1]. As technology advances and search engines evolve, no one can exactly know the way that personal data is collected. Even more, no one can control what data has already been collected and how these have been or will be used in the future, since search engines operate independently of the data subject. It is no coincidence that the Working Party[2] on Data Protection Issues of the European Union, on the one hand, emphasized the important role that search engines play in modern life and the information society and, on the other hand, highlighted the increase in the incidence of privacy violations[3].

The right to the protection of personal data in all its forms must also be considered within the above-mentioned framework. The protection of personal data, as a concept that is shaped in parallel with the rapid development of technology and the constant changes in the operation of search engines, is at the center of interest at the present time, where the role it plays both socially and economically is now being realized. In fact, according to recent studies[4], the digital economy, which relies on the collection, processing and storage of personal data, accounts for 1/5 of global GDP, with the Internet itself being the pinnacle of globalization, uniting both commercial and industrial sectors.

In view of the above, a reference will be made to the general need for the protection of personal data in the light of legislative developments at European level and, then, an extensive analysis of the right to erasure will follow.

As has become clear from the brief introduction, the right to erasure of personal data is now a reality that all bodies responsible for the processing of EU

[1] N.Zheng, A. Paloski and H. Wang, 'An Efficient User Verification System via Mouse Movements', Proceedings of the 18th ACM conference on Computer and communications security (ACM 2011) <http://dl.acm.org/citation.cfm?id=2046725> accessed 12 November 2019

[2] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 06/80

[3] Article 29 Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines' (2008) WP 148 <http://ec.europa.eu/justice/article-29/documentation> accessed 10 November 2019.

[4] Accenture Strategy και Oxford Economics , Digital Disruption: the Growth Multiplier, 2016, <https://www.accenture.com/us-en/insight-digital-disruption-growthmultiplier.asp> accessed 15 November 2019

citizens' personal data should respect. The right to erasure wants to serve a natural need to combat the eternal memory of the internet, allowing some data to be lost, as would be the case with the endlessly pervasive nature of the internet. In theory, this right seems to be an important “asset” of a democratic society, where every individual has the right to information, self-determination and autonomous development, without being haunted by the mistakes of the past. However, the implementation of the right presents several practical problems, such as infringing on other fundamental rights and freedoms.

This study will first examine the need for the protection of personal data and then the concept and nature of the right to erasure, as formulated by the European Union and its institutions, through the General Data Protection Regulation, but also through the Court of Justice's famous Google ruling, and the acceptance of these moves worldwide. Furthermore, this Dissertation Thesis will try to examine the “time” factor, as it is considered to be one of the most determining factors in finding the balance between memory and oblivion. Finally, there will be a research about the technological challenges that search engines face and how they can practically apply the right to erasure.

2. THE FUNDAMENTAL RIGHT TO DATA PROTECTION

2.1. The fundamental Right to Data Protection

The protection of privacy is a guaranteed right of the European legal order. It is perceived as an expression of European democratic society. The protection of personal data was born in the context of the right to privacy but is now a separate right, guaranteed both within the European Union.

The need for privacy was preceded and initially defined as the right to leave one's privacy at home. In its evolution, the right to privacy can be regarded as a sphere of personal privacy, in which society or other persons cannot be unjustly invaded and, thus, constitutes an expression of the right to free development of the individual and of human dignity. The development of technologies and the ever-easier dissemination of information have created the need for one to be able to control his/her personal information.

The protection of personal data become relevant when data started being processed. The massive processing of personal data that began in the late 20th century and the gradual domination of the Internet in all areas of life, led to the urgent need for separate legislative framework as it was immediately recognized by the European governments, that personal data issues could not be regulated by simple reference to the principles of privacy. Data protection has been a concern at an international level.

Some countries, such as Sweden[5], Germany[6] and France[7], adopted data protection legislation. Then, organizations such as the Council of Europe[8] and the Organization for Economic Co-operation and Development[9] played an important role in establishing data protection framework at State level.

The European Convention of Human rights first adopted 'the right to respect for private and family life' (article 8)[10]. For many years Article 8 ECHR was considered to offer sufficient safeguards to protect the private life of individuals. However, technological developments and all the changes they brought to life could not be foreseen. Another thing that could not be foreseen is how they would affect individuals' personal lives and their privacy rights. The use of computers, in both public and private sector, raised new, serious concerns[11] about whether these new technologies affected the rights of individuals.

These concerns lead to the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Convention 108). This particular text was of great importance because the term 'data protection' was used for the first time in a legally binding international document. The Convention

[5] 'The Data Act'.
[6] 'Act on Protection Against the misuse of Personal Data in Data Processing'.
[7] 'Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés'
[8] 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (28/01/1981)
[9] 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' [23/09/1980]
[10] Addopted in 1950.
[11] In 1968, the CoE Parliamentary Assembly highlighted that 'newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights'. Council of Europe - Parliamentary Assembly, 'Recommendation 509 (1968) - Human Rights and Modern Scientific and Technological Developments'

was focused on the protection of individuals' data and not on the right to privacy as it had been so far[12].

Despite the steps, undoubtedly, taken, it was clear that there were major mismatches in the protection of personal data between Member States. In the light of European integration, the European Commission pointed out the need for protection of the right to privacy and the need for no restrictions on the free flow of information between Member States.

Taking into consideration all the aforementioned, the European Commission, in 1990, issued a proposal for a 'Council Directive concerning the protection of individuals in relation to the processing of personal data'. This text formed the basis for the Data Protection Directive which was adopted in 1995[13]. The key idea behind the Data Protection Directive was a high level of protection of personal data between all Member States and the facilitation of free flow of information. The Directive harmonized many, different approaches to data protection rules throughout the European Union but, also, offered some flexibility to its application. A typical example of the flexible application of the Directive was the Lindqvist case in which the European Court of Justice stated, inter alia, that "*With regard to Directive 95/46, its provisions are necessarily relatively general, since it must be applied to a large number of very different situations. Consequently, contrary to what Mrs Lindqvist asserts, that directive correctly contains rules with some flexibility and in many cases entrusts the Member States with the task of regulating the details or choosing between alternatives*." [14]

2.2. From the Fundamental Right to Data Protection to the General Data Protection Regulation

All the aforementioned combined with the need for more legal stability and harmonization, in view of the internal market, have led to the need to find a

[12] European Union Agency for Fundamental Rights (ERA) and Council of Europe, Handbook on European Data Protection Law [Publications Office of the European Union, Luxembourg, 2018] p. 23-26 <https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en> accessed 19 November 2019

[13] Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

[14] Lindqvist v Åklagarkammaren [2003], Court of Justice of the European Union C-101/01 para. 83 et seq

law that would enhance accountability and create a fair system that would create confidence in data subjects, and would give them the necessary guarantees to feel more secure. This was the basis for the creation of the General Data Protection Regulation.

Free movement of people, goods, capital and services within the Union required free flow of data. This could not be achieved unless all Member States adopt and rely on a uniform high level of data protection. So, on January 25th, 2012, the European Commision proposed a reform to the existing legislation including the General Data Protection Regulation. The GDPR respected the principles of Data Protection Directive, while, at the same time, expanded them. Another important issue was that GDPR provided safeguards not only for the fundamental right to data protection, but also to other fundamental rights and freedoms, that are affected by data processing, such as freedom of expression, freedom of thought, freedom of association[15]. One of the main goals of the GDPR was to strengthen the rights of data subjects and ensure the existence of an effective and credible toolkit that will be available against any personal data breaches.

The GDPR introduced a separate provision on the right to erasure (Article 17) with the aim of further contributing to the empowerment of the individual as much as possible. This Article has caused a lot of discussion and will be the central topic in the following chapters. The first two chapters were necessary in order to explore the history and rationale of the right to data protection, in order to, finally, be able to place to right to erasure in a broader framework and provide a detailed analysis of how the right to erasure operates itself, its scope, its requirements etc.

[15] European Commission, 'Commission Staff Working Document Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) {COM(2017) 10 final} <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0003> accessed 15 November 2019

3. The Right to Erasure

"The Internet Never Forgets"[16]. This statement that touches on the essence of the way the internet works, coupled with the cumulative storage of personal information about each of us, lies at the heart of the debate on the right to erasure. By their nature, people are programmed to forget and remembering is the exception[17]

Since the advent of technology in our lives, this balance has changed. As people realize how easy is to get details about someone online (whether posted by themselves or posted by others) and as long as social media play a leading role in our lives, the right to be forgotten becomes of greater importance. In a society where everyone can 'see' the whole life of another person just by the touch of a button, one realizes that the right to delete information that no longer reflects one's image or has been made public without one's consent is becoming increasingly important. The Google ruling[18] of the Court of Justice of the European Union, have urged the right to be brought to the forefront, with the result that the debate has recently been rekindled.

However, the exact content of the right to erasure has not yet been clarified. Although it seems to be widely accepted as a concept, its practical and legal implications have not yet been thoroughly analyzed,[19] while the various terminologies used make the content of this 'new' right even more difficult to define. Moreover, it is not irrelevant that one of the problems associated with the right to be forgotten is that it causes emotional and instinctive reactions, despite legal analysis, especially considering that the debate on the right to be forgotten internationally has started relatively recently.

---

[16] J. Rosen, The Web Means the End of Forgetting, New York Times, June 2010, <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all&_r=0> accessed 23 November 2019

[17] V. Mayer-Schoenberger, Delete the Virtue of Forgetting in the Digital Age,[Princeton University Press, 2009], 2

[18] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014], Court of Justice of the European Union C-131/12.

[19] B.-J. Koops, Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice. [Tilburg Law School Legal Studies Research Paper Series, No. 08/2012], 2 <http://ssrn.com/abstract=1986719> accessed 23 November 2019

3.1. The Google Spain Case

The analysis of the right to erasure could not begin without a brief reference to the famous case of Google Spain, which is a benchmark for human rights in digital age.

On March 5, 2010, a Spanish citizen, Mario Costeja Gonzalez, filed a lawsuit with a Spanish newspaper, Google Spain SL and Google Inc., before the Spanish Privacy Authority (AEPD). The applicant complained that any internet user typing his name into Google's search engine would receive two Spanish newspaper publications about an auction order for his home. The applicant requested that the newspaper delete its name from the relevant publications and Google to remove its specific personal data from the results it provides to its users.

He claimed that enforcement proceedings against his home had been definitively terminated many years earlier and any reference to them has nothing to do with the present.

The Spanish Data Protection Authority has rejected the request for the Spanish newspaper, but has accepted it as far as Google is concerned. According to the Authority, the newspaper was not obliged to revoke the publications, as the latter had been legally published at the date of their publication. Instead, it held that search engines are processors of personal data and therefore Google Spain and Google Inc. were required to delete personal data at the request of the person concerned. The Authority based its decision on EU Directive 1995/46. Following this, Google Spain and Google Inc. appealed against the above judgment to the Spanish Supreme Court. The latter addressed the European Court of Justice with a series of questions for a preliminary ruling on the proper application of the Directive.

The questions referred for a preliminary ruling were, inter alia, whether Google falls within the meaning of the data processor and also whether, as a European company, it was subject to the provisions of the Directive. In the affirmative, the European Court of Justice was required to determine Google's responsibility as a data processor and to determine whether a citizen has the right to ask Google to delete his/her personal data.

The European Court of Justice ruled that Google is, in fact, a data processor, as it collects personal data, and defines the purposes and means of data processing. The Court also held that Google Spain is essentially a subsidiary of Google Inc. and therefore Google Inc. is subject to the EU Directive.

One of the highlights of the decision concerns the legal obligations of search engines, such as Google, in accordance with the Directive. The Court held in this regard that search engines have the right to process personal data where necessary to serve the legitimate interests of the data owner or third parties.

This right is not absolute. It can be restricted when the interests or fundamental rights of the subject are violated - in particular the right to privacy. The Court has held that the data subject has undoubtedly a legitimate interest in refusing to publish his data, even if the publication is not harmful to him any longer.

Therefore, the data subject - in this case Mr Costeja Gonzalez - may claim the erasure of his data if the information being published is inadequate, irrelevant or no longer relevant, or excessive for the purposes of the processing.

The Court ruled that Mario Costeja Gonzalez was entitled to request erasure of his data from Google, with the latter being required to delete it. This decision therefore recognized 'the right to be forgotten' for the data subjects and at the same time the obligation of the data holder.

3.2. The right to erasure after Google ruling

The aforementioned decision, in conjunction with other factors, triggered a debate about one's right to delete or not his/her personal data.

It is true that technological explosion and economic progress, in combination with globalization and commercialization have led to the loss of data control by the data subjects themselves. The CJEU recognized this fact and imprinted it in its judgment.

The Google Spain decision leaves the enforcement of the right to erasure in the hands of search engines. Data subjects who want links removed must file their requests to the search engine. Then, the search engine should examine the request and may either grant or deny. When a search engine denies a request,

the requester can choose to appeal to this decision to national data protection agency of each country[20], or to the national courts, by suing the search engine. If either the data protection agency or the court agrees with the data subject, then the search engine will be obliged to remove the specific data. If search engine's initial decision stand, the disputed content will remain accessible[21].

But, when a search engine grants a request, the path for those who are harmed by this decision is not really clear and unambiguous. A typical example of such a case might be the information-seeking public and the distributor of the content[22].

When a link is removed from search results, the search engine send a takedown notice to the content provider. This notice does not mention the person who requests for the erasure of the data, in order to protect their privacy. However, the notice mention which webpages will be deleted. The decision to send these notices based on the idea of some EU regulators who claim that the European Court's decision should be communicated and, thus, the right to be forgotten could emphasized[23].

However, whenever there is such a request the search engine is called upon to make a very important decision that will affect a wide range of actors involved, such as users seeking information, the publisher of the information and the data subject itself.

It is not a coincidence that Google's immediate response to the new requirements that Google Spain Case placed was to set up an Advisory Council to Google in the Right to be Forgotten[24]. The Advisory Council issued its Report in

---

[20] National data protection agencies were created in accordance with the Data Protection Directive by each European Union Member State. They exist to ensure the appropriate enforcement of the Directive in each country.

[21] S. Wechsler, The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten,[49 Colum. J.L.&Soc.Probs. 135,2015] p.142 <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/collsp49&id=142&men_tab=srchresults> accessed 25 November 2019

[22] Ibid. p. 142

[23] James Temperton, EU Demands 'Right to be Forgotten' be Applied Globally, [WIRED Nov. 26, 2014], <http://www.wired.co.uk/news/archive/2014-11/26/eu-right-to-beforgotten-extended> accessed 25 November 2019.

[24] Foundation The Advisory Council was set up in 2014 and the Members included: Luciano Floridi, Professor of Philosophy and Ethics of Information at the University of Oxford; Sylvie Kauffman, Editorial Director, Le Monde; Lidia Kolucka-Zuk, Director of the Trust for Civil Society in Central and Eastern Europe; Frank La Rue, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; Sabine Leutheusser-Schnarrenberger, former Federal Minister of Justice in Germany; Jos6-Luis Pifiar, Professor of Law at

January 2015. The Report included an overview of the Ruling, the nature of the rights at stake and, finally, the criteria for assessing delisting requests[25].

The Advisory Council made an effort to provide a comprehensive framework which Google, and generally, search engines could establish in order to evaluate the requests for erasure of personal data. However, as it was easily understood, the formation of such a framework is not easy. This framework, as it has since been shaped through the theory and jurisprudence of the national and European courts, we shall endeavor to examine in the following pages.

4. The concept of Personal Data

Personal data is defined as "*any information relating to an identified or identifiable natural person*"[26]. Similar is the definition found in European Directive 95/46/EC, which stipulates that personal data is any information that refers to a natural person whose identity is known or verifiable, and as a person whose identity may be verify is considered to be the person who can be identified, directly or indirectly, in particular on the basis of an identification number of one or more specific elements that characterize his or her existence as physical, biological, psychological, economic status.

The right to privacy and the right to the protection of personal data are often confused. The truth is that the two rights are related and even at the ECHR level they are protected by the same provision[27], while at European Union level the protection of personal data has become an autonomous fundamental right since its imprint in a separate article in the Charter of Fundamental Rights[28] and the judgment of the European Court of Justice decision in Case Promusicae[29] [30].

Universidad CEU and former Director of the Spanish Data Protection Agency ("AEPD"); Peggy Valcke, Professor of Law at University of Leuven; and Jimmy Wales, Founder and Chair Emeritus, Board of Trustees, WikimediaFoundation.
<https://static.googleusercontent.com/media/archive.google.com/el//advisorycouncil/advisement/advisory-report.pdf> accessed 25 November 2019

[25] Ibid. P. 7 et seq

[26] Article 4(1) GDPR. See, Article 2b of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Strasbourg, 28/01/1981] and Article 1b of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [2013]

[27] Article 8 of the European Convention on Human Rights.

[28] Article 8 of EU Charter of Fundamental Rights.

[29] Promusicae v Telefonica [2008], Court of Justice of the European Union C-524/06.

[30] Promusicae is a non-profit association of producers and publishers of music and audiovisual works. By letter of 28 November 2005, it applied to the Juzgado de lo Mercantil nº 5 de Madrid (Fifth Circuit Court of Madrid) for a

Regarding Internet, there are three cases related to personal data[31]: the first is the publication of personal data on a web site, the second is where a search engine displays results that refer to other websites that have published personal data and the third case is when an Internet user uses some of the features offered to him, such as searching, and in this context some data which can reveal his/her identity, such as the IP address, is automatically transferred to the provider of the corresponding service.

In the context of the protection of personal data, as technology evolves, concerns are raised about the risks of their misuse and whether the average user knows when and how they are violated. In particular, it is argued that the average user is unaware and unable to anticipate the risks that may arise from posting his personal data online. Usually, when they realize these dangers it is usually too late.

---

preliminary ruling against Telefónica, a trading company engaged in, inter alia, the provision of Internet access services. Promusicae has requested that Telefónica be required to disclose the identity and physical address of certain persons to whom the latter provides internet access and whose 'IP address' and the date and time of connection are known. According to Promusicae, these people use a file-sharing program (called "peer to peer" or "P2P") called "KaZaA" and allow access to their personal computer's shared directory of phonograms whose assets royalties belong to members of Promusicae. Promusicae has argued before the referring court that KaZaA users are competing unfairly and infringing their intellectual property rights. It therefore requested that the abovementioned information be disclosed in order to bring civil proceedings against the parties concerned. By order of 21 December 2005, the Juzgado de lo Mercantil nº 5 de Madrid granted Promusicae's application for preliminary injunction. Telefónica opposed that provision, claiming that, according to the LSSI, disclosure of the data requested by Promusicae is only permitted in criminal investigations or for the purpose of protecting public security and national defense and not in the context of civil proceedings or as a precautionary measure related to such a procedure. Promusicae has argued that Article 12 of the LSSI must be interpreted in accordance with several provisions of Directives 2000/31, 2001/29 and 2004/48 as well as Articles 17 (2) and 47 of the Charter, which do not allow Member States limit the obligation to disclose the relevant data only for the purposes pursued by the wording of that law. After a lot of discussion and many arguments the European Court of Justice ruled that: 'Directive 2000/31 / EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of the information society services, in particular e-commerce, in the internal market ("e-commerce directive"), 2001 / 29 / EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, 2004/48 / EC of the European Parliament and of the Council of 29 April 2004 on the with ep infringement of intellectual property rights, and 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the field of electronic communications (Privacy Directive) (electronic communications), do not require Member States to provide, in cases such as the one in the main proceedings, with the obligation to disclose personal data in order to ensure that voluntary protection of copyright in civil proceedings. However, Community law requires that those States, when transposing those Directives into national law, ensure that they are based on their interpretation which enables a balance to be struck between the various fundamental rights protected by the Community legal order. Furthermore, when implementing the measures transposing those directives into national law, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also not rely on their interpretation. which could conflict with these fundamental rights or with other general principles of Community law, such as the principle of proportionality'.

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

So, it is important to know what could or has been done with this data that, for whatever reason, has escaped control of the data subject. The subject should be able to know if and under what conditions he/she can delete the data or if he/she can somehow regain control of them. Can one just delete the data? What others options the data subject has? Can one totally be forgotten? This topic will be analyzed to the next chapter.

5. Conceptualizing the right to erasure

Academiccaly there is no uniformity in terminology when it comes to 'deleting personal data'. Some use the terms “right to oblivion”, “right to forget”, “right to be forgotten”, “right to delete” or “right to erasure" as synonyms[32], others vary the terminology they use[33]. It is not far from the truth to talk about terminological chaos. The term "right to digital oblivion" has also recently been introduced into the literature. In general, however, so far, not a uniform approach has been identified, that would clarify the problems of using different terminology and which, also, could clarify the substantial differences between the widely used terms. The interpretation given to the right to be forgotten is important, as the different meanings assigned to it require different technological means to achieve it[34].

5.1. The right to erasure

The right to erasure in its first aspect, refers to the deletion of information posted on the Internet either by the data subject or by third parties. It can be ‘seperated’ into two sub-aspects: on the one hand the right to erasure, enabling the deletion of personal data posted on the Internet with the consent of the individual, and on the other hand, the right to oblivion, which protects the

[32] See I. Inglezakis, The Right to Forget: A New Digital Right for Cyberspace, II.C, where he claims that the right of a person to delete personal data concerning him is equivalent to the right to be forgotten <https://www.lawspot.gr/nomika-blogs/ioannis_igglezakis/dikaioma-sti-lithi-ena-neo-psifiako-dikaioma-gia-ton-kyvernohoro> accessed 26 November 2019

[33] See, R. Weber, The Right to Be Forgotten: More Than a Pandora’s Box?, JIPITEC 2011 (2), 120 para 2,3, . that distinguishes between the right to forget and the right to be forgotten < https://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf> accessed 26 November 2019

[34] ENISA, The right to be forgotten-between expectations and practice [20 November 2012] <https://www.enisa.europa.eu/publications/the-right-to-be-forgotten> accessed 26 November 2019

individual from the possible consequences from the storage and processing of his personal data for a long period of time, which is founded and practiced over a period of time, so that the publication is no longer up to date[35].

The right to be forgotten aims to protect the reputation, identity and dignity of the person affected by the stay of information on the internet for longer than necessary. On the other hand, the right to erase data is intended to restore power between users and controllers, in the sense that since a person's consent to the processing of their data is rarely up-to-date, there must be a right to withdraw the consent of the user.

Erasure should be considered as a narrower concept than the right to be forgotten. The right to erasure does not necessarily relate to the passage of time, but aims to regain control over the subject of personal matters of data, regardless of time elapsed[36]. The purpose of the two rights is therefore different: the right to be forgotten, as a right derived from respect for the fundamental rights of privacy and personality, is based on the long tradition of balancing opposing interests, while the right to erasure can be seen as a procedural way of applying the substantive allegations of a breach of the provisions on personal data[37]. It is in a way clear that the right to erasure is more limited than the right to be forgotten.

5.2. The right to be forgotten

The right to be forgotten is really vague and is used more as an umbrella clause. The right to be forgotten is described as the right of individuals to have information about them deleted after a certain period of time[38].

The right to be forgotten has a broader scope and relates more to identity and self-determination. It has to do with "*information that with the passing of time becomes de-contextualized, distorted, outdated, no longer truthful (but not necessarily false), and through which an incorrect representation of the individual's identity is offered to the public*''[39].

[35] I. Inglezakis, The right to oblivion and its limitations [Sakkoulas Publications, Athens, 2014] p 83
[36] M. Ambrose and D. Ausloos, The right to be Forgotten across the Pond, JOURNAL OF INFORMATION POLICY 3 [2013]: 1-23, < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032325> accessed 26 November 2019
[37] Ibid.
[38] Ibid. p. 126
[39] Ibid. p. 127

Also, is often mentioned to the literature 'right to forget'. It encompasses the subjective right of individual's control over his/her personal data and memory of one's past. The latter is understood not from a psychological point of view, but has legal and social implications, including the right not to be confronted with details of his past that he would have preferred to forget[40].

In any case, the 'right to be forgotten' but also 'the right to forget' constitute the two aspects of the so-called 'right to oblivion', which considered to be much wider, as will be discussed in the next chapter.

5.3. The right to oblivion

The right to digital oblivion is a new and broad term that we find often both in literature and in case law. It relates to the publication of digital material data on the Internet and we could say that it is more a combination of different, autonomous rights, as it relies primarily on the right to the protection of personal data and, secondly, on the right to the protection of personality[41]. It mainly concerns personal information posted on a site, blog, social media and may have been reproduced by other media or displayed in search engine results.

According to one opinion, the right to oblivion applies only to data that has been posted by the same subject, or to those that have been processed with his consent[42]. According to another opinion[43], the right to digital oblivion is intended to give the person control over his/her digital world data, which basically are data stored online as well as organizational databases: 1) either

[40] B.-J. Koops, Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice. [Tilburg Law School Legal Studies Research Paper Series, No. 08/2012], <http://ssrn.com/abstract=1986719> accessed 23 November 2019

[41] M. Ambrose and D. Ausloos, The right to be Forgotten across the Pond, JOURNAL OF INFORMATION POLICY 3 [2013]: 1-23, p. 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032325> accessed 26 November 2019

[42] Ibid. p. 7

[43] N.N.G. de Andrade, Oblivion: The right to Be different….. from Oneself Reproposing the Right to be Forgotten, European University Institute - Law Department; UC Berkeley Law School, Berkeley Center for Law & Technology, [April 2012] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033155> accessed 28 November 2019

posted by the data-subjects that is, the so-called digital footprints[44], 2) either posted or reproduced by others, the so-called digital shadows[45].

Under both concepts, it is obvious that the right to oblivion relies on the fundamental respect for privacy. It aims to prevent potential harm to personality, and reputation of an individual.

Taking into consideration the aforementioned, there are two rights, of which the right to oblivion has to do more with the balancing of contradicting interests[46](re-balance power between data subjects and data processors) and the right to erasure has to do more with a violation of data protection principles.[47] The scope of the rights may be considered different "...*while the scope of the right to oblivion is limited to outdated data, the right to erasure potentially applies to any data whose processing violates data protection laws…"*[48]

Notwithstanding the conceptual differences that may exist between the above terms, for the purposes of the this Dissertation Thesis they shall be used as synonyms. Because their categorization has proved particularly difficult for legal circles and because they overlap to an extent, it is preferable to use them as a single term. In general, until the formulation of a uniform framework for their use by theory and jurisprudence, it is difficult to assert with certainty that we have different, distinct terms.

The fact that in this pepper the most commonly used term is 'right to erasure' has to do with the wording of Article 17 of General Data Protection Regulation (GDPR), as this right is not considered as a stand-alone piece of legislation, but in the light of the new pan-European legislative framework and within it. The second most common term used here is 'right to be forgotten' as it is commonly found in European case law. In fact, in this Dissertation Thesis none

[44] 'A person's public identified footprint is any information that they created which is online, widely available, and specifically linked to author's real name', S. Garfinkel and D. C. Naval Postgraduate School, Monterey, CA, USA, [February, 2009], <https://simson.net/clips/academic/2009.BL.InternetFootprint.pdf >, accessed 28 November 2019

[45] 'Data shadows refer to the information that a person leaves behind unintentionally while taking part in daily activities such as checking their e-mails, scrolling through social media or even by using their debit or credit card' P.N. Howard, New Media Campaigns and the Managed Citizen, Cambridge University Press, New York [October, 2005], p. 93

[46] A. Tamp and D. George, Oblivion, Erasure and Forgetting in the Digital Age, JIPITEC 5 (2) [2014] para. B II < https://www.jipitec.eu/issues/jipitec-5-2-2014/3997> accessed 28 November 2019

[47] Ibid.

[48] Ibid.

of the aforementioned conceptual distinctions will be adopted, as we consider that the development of each one is still at an early stage.

6. SCOPE OF THE RIGHT TO ERASURE

According to Aricle 17 of the GDPR "*1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).*

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in

accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims.''

It is true that the scope of the GDPR is quite broad. This is exactly one of the key innovations offered by the new Regulation. Because of the broad nature of the provision, it must be absolutely clear the territorial, material and personal scope of it. In this chapter, there will be a brief report on GDPR in general, but in conjunction with Article 17 which is the subject of this paper. It is vital to be absolutely clear what can be deleted, who can request the erasure and who is ultimately responsible to erase the information. If these concepts are not distinct then how do we know what we can erase or who is responsible for that erasure?

6.1. Material Scope

GDPR refers specifically to personal data. Article 3 (1) of GDPR defines the term 'personal data' as: 1) any information, 2) relating to, 3) an identified or identifiable, d) natural person. It is obvious that the information need to relate to an individual. Such examples are health, social status, pictures of people or houses[49], camera information or even accelerometer information[50]. Apart from the aforementioned, one of the most typical examples and commonly used technology systems for tracking personal data is tracking cookies, which are also considered to be personal data.

The information mentioned above need to relate to an identified or identifiable natural person. The Working Party highlights that the person might be identifiable because some information concerning him/her combined with other

[49] Belgian Privacy Commission, Frequently Asked Questions - Google Street View, <https://www.dataprotectionauthority.be/faq-themes/the-internet/google-street-view> accessed 2 December 2019.

[50] S. Hemminki, P. Nurmi and S. Tarkoma, Accelerometer-Based Transportation Mode Detection on Smartphones [ACM Press 2013] < http://dl.acm.org/citation.cfm?doid=2517351.2517367> accessed 02 December 2019

information will make the individual to be distinguished from others[51]. Also, the personal data protection provisions do not apply when dealing with anonymous data.[52]

It is beyond any doubt that the information must be relevant to a natural person[53]. Also, the GDPR explicitly exclude its applicability to legal persons[54]. Rights of legal persons are protected in other ways, whether in pan-European or national level. [55]

6.2. Personal Scope

Another important issue to determine the applicability of data protection law and, consequently, the right to erasure is the GDPR's personal scope. This question is vital in order to understand who can invoke the right, whose interests are affected and, finally, who can delete the data.

The first one to be protected is the data subject. Data subject is the natural person to whom personal data relates[56]. Data subjects enjoy equal rights under the umbrella of GDPR. But, there are certain categories of data subjects that may benefit more protection, such as minors or children (Article 8), and more vulnerable categories, like individuals with mental decisions or the elderly[57].

One more important question is who to ask for erasure. Mainly, the data controller[58] and the data processor[59] are sharing the responsibility in the light of exercising the right to erasure. The concepts of controller and processor is, in practice, quite vague and uncertain.

---

[51] Data Protection Working Party, Opinion 4/2007 on the concept of personal data, <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf> accessed 03 December 2019.

[52] Recital 26 GDPR '…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.'

[53] Recital 27 GDPR mentions that the Regulation "*does not apply to data of deceased persons. Member States may provide for rules regarding the processing of data of deceased persons*".

[54] Recital 14 GDPR states that "*This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons*".

[55] For example, by Company law or by Competition Law.

[56] See Article 4(1) GDPR

[57] See Recital 75 GDPR, which refers to vulnerable natural persons.

[58] Article 4(7) GDPR: "*…'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*…"

[59] Article 4(8) GDPR "…'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.."

From the perspective of the GDPR, a controller is the one who determines the purposes and the means of processing. The processor operates processing activities on behalf of the controller and it is usually a separate body/entity. It is really important to distinguish controller from processor in order to allocate liability in case of violation of personal data, determining the applicable law and, finally, ensure compliance with the requirements of data protection law. According to GDPR provision, requests for erasure of personal data are addressed to both processors and controllers.

In fact, the distinction between controller and processor requires a case-by-case analysis, taking into account the prevailing circumstances. In the cases we are considering in the present Thesis, search engines can be considered either controllers or processors, depending on the particular circumstances of each case.

7. CONDITIONS OF THE RIGHT TO ERASURE

One of the key aims of the right to erasure is to enable data subjects to regain control of their data. However, this does not mean that anyone can request erasure of data without any criteria, simply because the information is bothering him/her for some unspecified reason. This is exactly why Article 17 sets out the six (6) grounds for invoking the right to erasure. According to this Article there are some specific non-cumulative criteria for the application to erasure. As will become clear to the following pages, the preconditions for applying the right to erasure are closely related to other provisions in the GDPR.

The first ground (Article 17(1)a) for requesting erasure is that the data subject believes that the data are no longer necessary for the purposes which they first collected. This is the so-called purpose limitation principle[60] [61] and is closely linked to Article 5(1)b GDPR. From the abovementioned provisions it follows that the purposes for data processing need to be specified, explicit and legitimate. When personal data is 'inadequate, irrelevant or unnecessary'[62] to

[60] Purpose limitation principle in not only found in GDPR but has already been specified by Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation,<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf > [02 April 2013, WP 203] p. 15-20.
[61] The purpose limitation principle also features in the Charter (Article 8(2)).
[62] So-called data minimization principle established in Article 5(1)(c).

achieve those specific and in advance known purposes, the data subject can ask for erasure.

The second ground to erasure is withdrawal of consent. Controllers may process personal data only if they have a '*freely given, specific, informed and unambiguous indication of his/her wishes be which he or she, by a statement or by a clear affirmation action, signifies agreement to the processing of personal data relating to him or her*.'[63] Requesting erasure under 17(1)b, provides that controller had obtained validly the consent of data subject in the first place.[64] Even if a data subject withdraw his/her consent, the controller might continue processing the same personal data on the basis of another lawful basis[65].

The third situation referred to in Article 17 which grants data subjects the right to erasure is upon a successful exercise of the right to object pursuant to Article 21 (1). There is a different scope between the two Articles. Article 17 aims to the prevention of processing of certain data which for some reason cannot be stored or in any other way processed by the controller while Article 21 aims to the prevention of further processing of specific data. This provision actually attempts an (informal) opportunity for the controllers to choose between the two, weighing each time their particular circumstances and interests. There must be a balancing of the profiling for the controller himself, on the one hand, and on the impact of the profiling on the data subjects themselves, on the other hand.[66]

The fourth situation in which data subject can invoke the right to erasure is when data have been unlawfully processed[67]. Lawfulness means to have a lawful ground for processing data under Article 6(1) GDPR. The requirement for having a lawful ground is closely linked to a specific processing operation. If, in this particular operation there is no lawful ground, there is a basis for applying the right to erasure.

[63] Article 4(11) GDPR and Recital 32.
[64] In fact, it is very difficult for the controller to obtain the consent of the subject as there are many requirements that must be met in order for the consent given to be valid.
[65] For example, on the ground of controllers' legitimate interests (Article 6(1)f).
[66] Article 29 Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, (06 February 2018, WP251Rev.01)< https://iapp.org/resources/article/wp29-draft-guidelines-on-automated-individual-decision-making-and-profiling> p. 18-19
[67] One of the basic principles underlying GDPR is that of fair and lawful processing of data.

Furthermore, data subjects will have the right to erasure when such erasure is required in order to comply with a legal obligation in Union or Member State law to which the controller is subject. Three conditions must be met: a) necessity, b) a legal obligation and c) controller must be subject to that obligation. There is no specific reference but it is implied that there must be an urgent situation. GDPR does not clarifies what kind of legal obligation looks like and the term is quite vague, but Article 17(1)e requires the relevant legal obligation to be applicable to the data controller.

Finally, the sixth and last ground aims to protect children. It grants data subjects the right to request for erasure of personal data when those data have been collected in relation to the offer of information society services directly to a child. It is crucial that the personal data was collected when the data subject was a child. The justification for such a provision is the fact that children need extra protection with regard to their personal data, because they may be less aware of the risks and safeguards about the processing of personal data.

According to the aforementioned, it is obvious that GDPR sets the grounds for erasure but, whether the data subjects' request will be parsed and the data erasure will follow is a question that depends on many factors, which we will analyzed in the following chapters.

8. BALANCING AND CONFLICT WITH OTHER RIGHTS

Although the 'right to be forgotten' is of undeniable value and importance, it raises both practical and substantive issues, in relation to its conflict with other fundamental rights. That is why its conceptual distinction and the scope of its application, as mentioned above, are very important to be defined as clearly as possible. The right to be forgotten falls within the protective framework of Article 8 (right to respect for private and family life) and, this right is exercised with respect to the content of other opposing rights. According to Article 8(2) of the ECHR, "*The exercise of this right shall not be invoked by any public authority unless it is in accordance with the law and is necessary in a democratic society ….. to protect the rights and freedoms of others*". Full enjoyment of the right to be

forgotten will almost always be in tension with other fundamental rights and freedoms. Therefore, it is necessary to properly balance rights in the application and interpretation of Article 8 ECHR and Article 8 of the Charter[68]. Furthermore, it has been held that the fundamental right to the protection of personal data "*is not absolute, but must be taken into account in relation to its role in society*[69]".

The balancing of opposing rights seems particularly difficult for a number of reasons. First of all, fair balancing cannot be defined at abstract level and its application should be considered by the particular context of each case. Indeed, when we have to do with fundamental rights it is difficult to decide in absolute terms and without second thought that one fundamental right or freedom overrides another.

Fair balancing seems to be the preferred and appropriate mechanism to resolve conflicts between fundamental rights and freedoms. Some guidance on how to balance the rights involved can be found in Article 52 of the Charter, which sets the conditions under which the rights and freedoms can be limited and to what extent this limitation should be tolerated by the data subjects and by the legal system itself. An overview of the Article shows that there are four prerequisites for the restriction to be lawful. Limitations must be: a) provided for by law, b) respect the essence of the relevant right and/or freedom, c) comply with the principle of proportionality and d) be necessary and genuinely meet objectives of general interest recognized by the Union, or the need to protect the rights and freedoms of others.

As can be seen from the above, all the involved concepts are particularly vague and difficult to understand and apply. In particular, as regards the issue of limiting the core of the right, many views have been formulated from time to time. The European Data Protection Supervisor in an effort to facilitate fair balancing and to resolve the increasingly complex conflicts mentions that: "*the*

[68] See, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado [24 November 2011] Court of Justice of European Union Joined Cases C-468/10 and C-469/10

[69] See, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [9 November 2010] Court of Justice of European Union Joined Cases C-92/09 and C-93/09, para. 48

limitation goes so far that it empties the right of its core elements and thus prevents the exercise of the right"[70].

According to the guidelines that European Data Protection Supervisor sets, there are some important steps to be taken into consideration, to assess the validity and necessity of the measures taken, in relation to the limitation of the rights and freedoms. There need to be a description of the measure proposed, an identification of fundamental rights and freedoms limited by the processing of personal data, a determination of the objectives of the measures and, finally, to choose an option that is effective and least intrusive[71].

Fair balancing is an idea that exists throughout the GDPR. GDPR aims to protect personal data and any limitation to that right will be scrutinized by the framework sets out in Article 52(1) of the Charter and according to the requirements which the regulation itself sets out. For limitations to the right to data protection GDPR foresees some clear justifications such as national security, public interest, defence etc. A wide range of provisions ensure a fair balance between rights, throughout the GDPR. First of all, the most notable is Article 5(1) (principles relating to processing of personal data), but, also, Article 9 and 10 (processing of special categories of personal data) Article 12 (transparent information, Article 6(1) (compliance with a legal obligation) Article 21 (right to object) and others.

We could claim that fair balancing operates as a principle underlying the whole framework of GDPR. Fair balancing in the GDPR implies personal data should not be processed in such a way which unreasonably infringes the fundamental rights and freedoms of the data subject or third people[72].

This chapter examines the conflict of the right to be forgotten with other rights and the efforts made by both theory and Courts to achieve a fair balance.

[70] European Data Protection Supervisor, Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit', [11 April 2017] <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf> accessed 08 December 2019

[71] Ibid. p. 9 et seq.

[72] See, Coty Germany v Stadtsparkasse Magdeburg [2015] Court of Justice of the European Union C-580/2013, Maximillian Schrems v Data Protection Comissioner [2015] C-362/2014

Without the list being exhaustive, we believe it captures the greatest conflicts, as they have been found until today.

9. RIGHT TO BE FORGOTTEN IN RELATION TO FREEDOM OF EXRESSION

Freedom of expression is enshrined in Article 10 para. 1 of the ECHR, Article 19 para. 2 of the International Covenant on Civil and Political Rights and Article 19 of the Universal Declaration of Human Rights, as well as national regulatory texts. At European Union level, freedom of expression is enshrined in Article 11 of the Charter of Fundamental Rights, which corresponds to Article 10 ECHR ('Freedom of Expression and Information'). This right includes freedom of opinion, freedom to express views through Internet, television, books, published articles and art, as well as freedom to receive or impart information and ideas without interference by the authorities.

Freedom of expression, as protected by Article 10 § 1 of the ECHR, forms the basis of a democratic society[73]. The restrictions legally enforced on the right to freedom of expression as enshrined in all the above texts cannot go beyond what is provided for in Article 10 (2) of the ECHR. First, they must be provided by law and secondly, they must be necessary in a democratic society for protecting rights and freedoms of others.

Nowadays, with the important role that the Internet plays in expressing opinions, it is much more urgent to see how the right to data protection is defined in relation to freedom of expression. For the press, the freedom to transmit and receive information, and the guarantees provided therein, are of particular importance. Press has a duty to impart information and ideas relating to the public interest[74]. Therefore, any measure restricting access to information which the public is entitled to receive must be justified on particularly compelling grounds[75]. In fact, in the judgment of the Editorial Board of Pravoye Delo and

[73] Handyside v The United Kingdom [1976] European Court of Human Rights (Series A No 24,5393/72). Para. 43 et seq

[74] The Observer and the Guardian v The United Kingdom [1991], European Court of Human Rights (Series A, No 216, 13585/88) para. 59.

[75] Timpul Info-Magazin and Anghel v. Moldova [2008], European Court of Human Rights (42864/05) para. 26 et seq

Shtekel v Ukraine[76], the Court recognized that Article 10 of the ECHR should be interpreted as imposing a positive obligation on Member States to establish an appropriate regulatory framework to ensure effective protection of freedom of expression for online journalists.

The Internet poses a lot of risks to both data protection and freedom of expression, which sometimes overlap and create legal issues that are even more problematic to their nature and much more difficult to resolve them.

The Special Rapporteur on the United Nations Frank La Rue in the 2011 report on promoting and protecting freedom of opinion and expression[77], points out that the lack of adequate protection of privacy and personal data is an obstacle to the unhindered exercise of the right to freedom of expression. The lack of anonymity and the ability of governments and states to access user information are factors that undermine not only the right to privacy, but also freedom of expression, as users self-censorship, thus blocking the free online circulation of ideas and information. This is another interesting approach about how individual rights affect and ultimately shape each other.

There are several cases of Internet users posts that raise issues of conflict between the two rights we are considering. First of all, the user posts something on a webpage and subsequently changes his/her opinion and seek to delete it. This case is the easiest and raises fewer problems, as almost all online services offer this right. However, we should highlight that there is a great distance between deleting spam from a website and deleting it from the Internet generally[78]. Another case is when the user posts something and someone else copies it and posts it himself/herself on his/her own website. In this case, if the original user requests the second to delete the content and the second user refuses to do so, then the only solution is to refer the first user to the web platform where the content is stored and ask for erasure. However, the online platform that is required to erase data from someone else's website based solely

[76] Editorial Board Of Pravoye Delo and Shtekel v Ukraine [2011], European Court of Human Rights (33014/05)
[77] Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Meeting of the Security Council in Arria format on:«Protecting journalists» [2013] <https://www.ohchr.org/Documents/HRBodies/SP/StatementSRFreedexProtectingJournalists13Dec2013.pdf> accessed 11 December 2019.
[78] This happens because of the use of cookies.

on one user's request is in a difficult position to judge between the right to privacy of the first user and the freedom of expression of the second user. In this particular case there are questions also arise as to whether we want such decisions to be made by online platforms. Another case is when a user posts content about someone else, without being defamatory, so that the relevant criminal law can be applied. When it comes to truthful information which the data subject do not wish to become known or at least not further known, the conflict between freedom of expression and the right to privacy is inevitable and the legislator, as well as the judge, is required to balance those contradicting interests.

As one can see from all the foregoing analysis, balancing the conflicting interests between the right to be forgotten and the freedom of expression is not easy and made more difficult by the fact that the right to be forgotten is still a vague concept[79].

As it is obvious, court decisions and legal texts are shaped in the light of technological developments. The GDPR is the only legal document at EU which governs the interaction and interconnection between Articles 8 and 11 of the EU Charter of Fundamental Rights. In this context, courts at both national and European level are called upon to play a particularly difficult role.

As the current case-law has developed it seems that there are some factors that play an important role in this difficult balance between different rights. Particularly important are the persons whose data are processed who happen to be public persons. Public persons means persons who hold public office and/or use public money or even all those who play a role in public life, such as politicians, athletes, actors, celebrities or any kind of public figure generally[80]. Furthermore, important for the right to be forgotten is the element of

[79] M.Corrales, M. Fenwick and N. Forgo, New Technology, Big Data and the Law [Springer Nature Singapore, 2017] p. 1-3

[80] Adams M. Kate, (Re)Difing Public Officials and Public Figures: A Washington State Primer.(Archive) *Seattle University Law Review*. Seattle University School of Law. Vol 23:1155-2000. <https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1646&context=sulr> accessed 12 December 2019.

time[81], in the sense that it can change the balance between opposing interests: information that has been lawfully published at some point may no longer be lawful over time[82].

A key principle that follows the aforementioned is that the right to data protection and freedom of expression must be treated equally. A fair balance must always be sought and an ad hoc judgment must be made. Which right prevails in any particular case depends on the specific regulatory value that each right holds under each particular circumstance. European Courts are oriented towards this point of view as shown by the case-law rulings.

In Von Hannover v. Germany case[83], the Court was asked to rule on whether the disclosure of private photos of Monaco Carolina violated Article 8 of the ECHR. The Court held that the decisive criterion for the distinction between the right to privacy and data protection of the subject and freedom of the press is whether the publications contribute to a debate of general interest. On 24 June 2004, the Court unanimously ruled that there was a breach of Article 8. Furthermore, it accepted that scenes from daily life, involving activities such as engaging in sport, out walking, leaving a restaurant or on holiday were of a purely private nature and there were not of public interest.

In case of Osterreichischer v Austria[84] the European Court of Human Rights found that the Austrian authorities had acted in violation of the right to freedom of expression. The case concerned a reaction to a news item on the Austrian public television channel (Österreichischer Rundfunk). In a news programme broadcast by the channel in 1999, a picture was shown of a person, Mr. S. Mr. S. had been released on parole a few weeks earlier. He was convicted to eight years imprisonment in 1995 because he had been found to be a leading member of a neo-Nazi organisation. At the request of Mr. S., the Austrian courts prohibited Österreichischer Rundfunk from showing his picture in connection with any report stating that he had been convicted either once the sentence had been executed

[81] M.Ambrose and J. Aulsloos, Timing the Right to be Forgotten, A Study into 'time' as a factor in deciding about retention or erasure of data [2015], < http://archive.ceu.hu/publications/korenhof/2015/43831> accessed 11 December 2019
[82] Ibid p. 2
[83] Von Hannover v Germany [2004], European Court of Human Rights [No 59320/00]
[84] Osterreichischer v Austria [2007], European Court of Human Rights, [No 35842/02]

or once he had been released on parole. The courts found that the publication of Mr. S.'s picture, in that particular way, had violated his rights.

In Mosley v United Kingdom Case, Max Mosley, a former president of the FIA (Fédération Internationale de l'Automobile**,** an association to represent the interests of motoring organisations) filed an application for breach of Articles 8 and 13 of the Convention of the European Convention on Human Rights, claiming that United Kingdom failed to impose a legal obligation against News of the World (newspaper published in the United Kingdom from 1843 to 2011) to notify him before the publication a story regarding his private life. In this case, judges ruled in favor of United Kingdom. The court ruled that although there was a clear obligation to ensure that personal privacy was protected, there were existing protections in place, including the options of referral to the Press Complaints Commission (regulatory body for British printed newspapers and magazines) and the possibility of seeking (through it) civil damages.

The CJEU both in Lindqvist[85]and in Satamedia[86]case decided that controllers could rely on freedom of expression derogations. In Lindqvist case, European Court of Justice, decided that referring to particular persons on an internet page and identifying them by any way (by name or by another characteristic) constitutes processing of personal data by automatic means and is now allowed. In Satamedia case, found no violation of the right to freedom of expression where Finnish courts and authorities had prohibited two companies from processing personal tax data in the manner and to the extent that they had. The Court held that restrictions to the freedom of expression were compatible to law and aimed to protect personal data of taxpayers.

10. RIGHT TO BE FORGOTTEN IN RELATION TO THE RIGHT TO HISTORICAL MEMORY

One recent point of view is that the right to be forgotten may not be compatible with the right to preserve the collective memory of humanity. In one

[85] Bodil Lindqvist v Åklagarkammaren i Jönköping [2003],European Court of Justice, C-101/01
[86] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [2015]. European Court of Justice, C-73/07

sense, deleting the past can affect mankind's future. In fact, it is difficult to build the future without retaining memories of the past, as the events of the past are what have brought us here[87]. The past passes and there is no way to change it. But, humanity needs points of reference in order to be able to move forward, while the need for one to know their roots, their past and be able to place themselves within a historical context is a fundamental need of every person in today's rapidly changing societies.

Actually, this issue is not just about important events or persons, but also about 'every day people', either through an individual approach (family history/family memory) or collective (social, journalistic, economic history of their country/continent). So, it is common argued that by deleting personal data from the Internet (files, links etc) it is argued that the remaining information becomes incomplete and does not reflect an accurate image of reality. The truth is that this view contains a great deal of reality. But, on the other hand, there is the opposite opinion: societies need to forget in order to evolve and survive. The idea that people could remember everything, anytime seems to be a nightmare, as it fits into a society where people would stay attached to the past.

The person seeking to erase his data in an effort to define himself/herself in a different way or even 'reinvent' himself/herself is essentially trying to meet social expectations, needs and desires, which form part of the society in which the data subjects lives. This erasure not only leads to a different picture of a particular person but also to a different 'reading' of social reality over a specific period of time.

The need to reconcile a person's right to self-determination and the right to a true record of reality and history is a complex problem and highlights the complex relationship between memory, history and politics, which requires co-operation and finding mutually acceptable solutions among historians, politicians, social and legal scientists[88].

[87] G. Della Morte, International Law between the Duty of Memory and the right to Oblivion, [2014 International Criminal Law Review 14], p. 427 et seq <https://heinonline.org/HOL/Page?public=true&handle=hein.journals/intcrimlrb14&div=26&start_page=427&collection=journals&set_as_cursor=0&men_tab=srchresults> accessed 18 December 2019

[88] A. Gliszezynska-Grabiaw, Memory Laws or Memory Loss? Europe in search of its Historical Identity Through the National and Internationa Law, [34 Polish Y.B. Int'L, 2014]

The European Parliament has also embraced this approach, when adopting the Proposal for a Regulation, adding a new article, which provides that personal data may go beyond what is necessary to fulfill the purposes of the initial processing for which they have collected for a period of time, to be processed by file services, which have as their primary duty or legal obligation to collect, store, classify, notify, exploit and the dissemination of archives for the public interest, in particular with a view to safeguarding human rights for historical, statistical or scientific purposes. All these must be taken into consideration in accordance with the rules laid down by Member States in the field of access, disclosure and dissemination of administrative or archival documents, and in accordance with the provisions of this Regulation concerning in particular consent and the right to object[89]. Finally, GDPR includes an exemption in paragraph 3 which allows a derogation from the grounds set out in paragraphs 1 and 2 for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Can deleting data deprive Europeans of their historical past and identity? This is a very difficult question and the answer is still quite vague. The ECHR has had to consider on several occasions the interpretation of the past. In the case of the Editorial Board of Pravoye Delo and Shtekel v. Ukraine[90], the Court stated that the Internet is an information and communication tool very different from the print media. The risk of damage to content on the Internet in the exercise and enjoyment of human rights, is clearly greater than that posed by the Press. Consequently, the policies governing the reproduction of print media and the Internet equivalent may differ, since the latter should be adapted to the specific characteristics of the technology in order to safeguard and promote the rights and freedoms concerned[91].

<https://heinonline.org/HOL/Page?public=true&handle=hein.intyb/polyeai0034&div=10&start_page=161&collection=intyb&set_as_cursor=4&men_tab=srchresults> p. 163 accessed 31 December 2019

[89] Article 83a of the European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014AP0212> accessed 18 December 2019.

[90] Editorial Board of Pravoye Delo and Shtekel v. Ukraine [2011], European Court of Human Rights [No 33014/05]

[91] Ibid para. 63

There are many cases in which the ECHR had to balance between historical memory and the standards of human rights protection provided by the European Convention. Such an example is the PETA Deutschland v Germany Case[92]. In that case, the ECHR ruled that Germany did not violate Article 10 of the European Convention on Human Rights when it prevented the publication of posters that compared images of caged animals with those of concentration camp prisoners. The applicant was forbidden by German Courts to launch an advertising campaign under the slogan 'The Holocaust on your plate'. The case originated when Jewish Holocaust survivors requested an injunction preventing the dissemination of posters highlighting the similarities between the mistreatment of animals and the suffering of victims in Nazi camps. The ECHR found that the injunction was a justifiable restriction as it sought to protect Jewish Holocaust survivors and that the German courts had properly struck a balance between freedom of expression and the obligation to respect historical memories and the reputation of others.

From all the aforementioned, we conclude that the legal framework should balance the opposing interests, protecting not only personal data but, at the same time, maintaining credible and authentic sources of history. Last but not least, we must not overlook the power of the Internet and its ability to shape the flow of events.

11. RIGHT TO BE FORGOTTEN IN RELATION TO THE FREEDOM TO CONDUCT A BUSINESS

The ruling of the European Court of Justice against the Google in Google Spain case highlighted the problems that the existence and protection of the freedom to conduct a business can create.

After the conviction of the company, thousands of requests have so far been received for the removal of results which individuals regard as outdated or unrealistic. Each request needs to be carefully considered and this requires a great deal of effort on the behalf of companies. Both colossal companies like Google and smaller businesses, like blogs, sites, online newspapers etc, need to

[92] PETA Deutschland v Germany Case [2012], European Court of Human Rights, [No. 43481/09]

be very careful to the examination of these requests. The enormous amount of information available on the Internet makes it impossible to control it. It, also, makes necessary for each request to spend time verifying and cross-checking data to determine whether this information no longer needs to be available. This has as a result that each company should have a person who will be entrusted with this difficult task. He/she must examine carefully all relevant information, balance the opposing interests and decide about the future of the content in dispute, while there is a risk of imposing huge fines. In this way the Internet Service Provider (eg search engine or social networking site) is overburdened as it is required to prove that there are specific reasons for keeping the information available.

Article 16 of the EU Charter provides for freedom to conduct a business according to Union Law and national laws. The right actually endorse a commitment to a certain economical and political model, which promotes and safeguards the ability of people within the Union to be entrepreneurial[93]. According the CJEU the freedom to conduct a business includes the freedom to exercise an economic or commercial activity and free competition among others[94]. In fact, there is a great deal of discretion in interpreting this freedom.

In view of the aforementioned, it is clear that questions arise as to whether this interferences with the internal issues of the respective Internet Service Provider is acceptable and, whether, they ultimately affect the freedom to conduct a business. Does the right to erasure make it effectively impossible for the economic operator to conduct its business?

According to the CJEU, Article 16 is considered to be violated, when there are no viable alternatives and the business is effectively deprived of its freedom to contract[95]. Interests of the Internet Service Providers may be negatively affected to the extent the actual operation of erasure is disproportionately

[93] S.Peers, T. Hervey, J. Kenner and A. Ward, The EU charter of fundamental rights: a commentary [Hart Publishing 2014] p. 438 et seq,< https://www.bloomsburycollections.com/book/the-eu-charter-of-fundamental-rights-a-commentary/> accessed 20 December 2019

[94] Spain and Finland v Parliament and Council [2004] Court of Justice of the European Union C-184/02 para. 51-52.

[95] AffishBV v Rijksdienst voor de Keuring van Vee en Vlees [1997] Court of Justice of the European Union C-183/95.

difficult. This may happen when, from a technical perspective, erasure requires significant resources (eg. special technological equipment).

As it becomes obvious, the crucial point is whether the right to erasure constitutes a justified interference to the ISS provider's freedom to conduct a business. In practice, this problem can be solved by balancing opposing interests and applying the principle of proportionality on a case-by-case analysis.

12. RIGHT TO BE FORGOTTEN IN RELATION TO THE RIGHT TO INTELLECTUAL PROPERTY

Article 17 of the Charter protects both physical and intellectual property. In practice, many conflicts have been brought before the CJEU that relate to Internet Service Providers being asked to share the data of users suspect of IP infringement with rights holders.

Promusicae v. Telefonica[96] is one one the most famous cases. Promusicae, is a non-profit organization composed of producers and publishers of musical and audiovisual recordings. Promusicae asked the ECJ to order Telefonica (ISS), to reveal personal data of its users. The reason for that was that Telefonica's users were allegedly accessing the IP-protected work of Promusicae clients without permission. The Court examined whether Member States, should impose obligations to Internet Service Providers in order to ensure effective protection of intellectual property rights. The Court found that Member States should not impose such obligations for the purpose of initiating civil proceedings for the protection of IP rights, and that, Member States must strike a fair balance between the rights at stake.

Other well-known cases of this nature are Scarlet Extended v Sabam[97] and SABAM v Netlog[98]. The ECJ, in many of those cases found that, in order to ensure that there is a right to a remedy against persons whose intellectual property rights have been violated by Internet Service Providers of their users, the

[96] Promusicae v Telefonica de Espana [2008], Court of Justice of the European Union, C-275/06. See N 30.
[97] Scarlet Extended SA v Sabam [2011], Court of Justice of the European Union, C-70/10
[98] SABAM v Netlog NV [2012], Court of Justice of the European Union, C-360/10

operator of an online platform (marketplace) may be ordered to take measures to make it easier to identify clients[99].

In all these cases the Court attached great importance to the personal data of users of Internet Service Providers by not allowing their behavior to be controlled and their data to be transferred without safeguards. Zooming into the right to erasure in particular, we can say that Article 17 Charter might be invoked against erasure requests that would effectively 'remove traces' of data subjects' IP infringements (e.g. asking internet access providers to erase IP-logs). The answer to this is Article 17(3)e under which, unless there is an ongoing investigation, it will not be possible to block erasure requests because of the right to intellectual property. At this point it is worth mentioning the Recital 63 GDPR, which highlights the elements mentioned above. According to this provision, access rights should not affect intellectual property but also, intellectual property cannot be used as an excuse to refuse access.

In conclusion, it is acceptable that IP rights could justify access restrictions. But, intellectual property should not be used as a 'panacea' to reject all or most of the erasure requests. Article 17 should have a substantial impact on the particular case in the light of accountability and proportionality.

13. TIME AS A CRITERION ABOUT ERASURE OR RETENTION OF DATA

As it is clear from all of the aforementioned there are many arguments for both the erasure and the retention of personal data. But in order to make a final decision on whether or not to erase, a balance must be made between different factors. European case law seems to take into consideration the time factor.

In Delfi AS v Estonia case[100], the ECHR stated that the spread of the Internet increases the possibility that information once made public will remain public and circulate forever, regardless of the data subject's will. In Editions Plon v. France case[101] the applicant, a publishing company and the authors of a book which contained information about former French President Mitterrand's secret

[99] L'Oreal v eBay [2011] Court of Justice of the European Union C-324/09.
[100] Delfi AS v Estonia [2015], European Court of Human Rights, No 64569/09
[101] Editions Plon v. France [2004], European Court of Human Rights, No 58148/00

health problem, were stopped through a court injunction by the family of President Mitterrand from distributing the book. The applicant filed a complaint relying on Article 10 of the European Convention on Human Rights and alleged that the order forbidding it to continue distribution of the book had infringed its right to the freedom of expression. The Court found that there had been no violation of Article 10 and held that the subsequent ruling to ban the book was in violation of Article 10 because it no longer met a pressing social need nine months into the Presidents death. Hence the interference with applicant's right to freedom of expression was no longer justified.

As it is obvious that 'time' is a crucial factor about the retention or erasure of certain information. The information one chooses to share at a particular time of his/her life does not necessarily mean that they want to follow him/her forever. This phenomenon can take a large toll on both personal and professional life. The example of the "Drunk pirate" mentioned very often in the literature[102]: Stacy Snyder, a graduate of the pedagogical school, posted on a social network page a photo of her wearing a pirate hat and holding a plastic cup, while writing in the caption that accompanied the photo the phrase "drunken pirate". The school in which she did her internship found that she promoted the consumption of alcohol by minors and her behavior was inappropriate and unacceptable for the University. As a result, she was not allowed to complete her internship and did not receive a degree in pedagogy. Snyder argued that she had the right to post the photo, but the Court rejected her claim on the ground that she was a civil servant and her plea was not in the public interest. After the publicity of this case, many questions were raised about how a post can affect a person's life after years and if it is fair to determine some important choices in data subject's life or if there should be a way for that 'mistake' to be forgotten.

Actually, the right to be forgotten is invoked in situations where an individual's personal life is publicly exposed. A careful balancing exercise with

[102] Snyder v. illersville Univiversity [2008] U.S. District Court of Pennsylvania, Case 2:07-cv-01660-PD

other fundamental rights will be imperative. In striking this balance, time may play a determinative role[103].

It is hard to draw clear conclusions about the role of 'time' within data protection context. However, we can say that, on the one hand, time is a factor adding or removing weight to the request to remove personal data while, on the other hand, time can play role as the marker of the tipping point when the grounds for retention no longer hold and erasure of the data should follow[104]. Generally, it is an undisputable fact that the older information is, the less valuable retaining it is.

Another important thing that should be considered in combination with time is the purpose limitation principle. Once the stated purpose is reached, there is no longer a legitimate ground for data retention, regardless of time. From this time data retention is no longer legitimate.

In conclusion, it is true that digital information sources have 'eternal memory'. But, this memory requires the implementation of a form of a digital forgetting. Balancing these interests is quite difficult but it is a fact that 'time' is a factor that supports forgetting, when enough time has elapsed since the publication of an information[105].

14. TECHNOLOGICAL CHALLENGES IN APPLYING THE RIGHT TO BE FORGOTTEN

Beyond the legal dimensions of the right to be forgotten, a brief reference should also be made to some technological issues that are inextricably linked to the erasure of personal data.

The fundamental technological challenges in applying the right to be forgotten lie especially on the following: 1) whether people are allowed to identify and locate stored personal data related to them, 2) whether identifying

[103] P. Korenhof, J. Ausloos, I. Szekely, M. Ambrose, G. Sartor, R. Leenes, Timing the Right to Be Forgotten A study into "time" as a factor in deciding about retention or erasure of data [CPDP 2014] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436436> accessed 24 December 2019.
[104] Ibid. para 3.3.
[105] Ibid. para. 6

all copies of information and 3) determining whether the person who asks for the erasure has the right to do so.

According to the first two issues should be briefly mentioned: The enforcement of the right to be forgotten is depend on the characteristics of the information system in question[106]. In essence, this is only possible in so-called "closed"[107] systems where information is processed, stored and transmitted in a particular context, preventing data from being distributed to sites where erasure cannot be accomplished. Information coexists in a way that the right to be forgotten can be enforced, each request is authenticated and recorded, and data and/or information is communicated directly to individuals and organizations. Systems such as corporate and public networks seem to meet these standards. On the other hand, in an "open" system [108]such as the Internet, public data can be accessed by interested members with online identities that cannot be shared with natural persons. These interested members have the ability to redistribute the information to non-confidential persons, resulting in mass copying of data. In such a system, there is no appropriate technical approach to enforce the right to be forgotten. This case is quite common on the Internet, especially when personal data is included on social media, blogs etc.

In addition, to personal data being processed in an open or closed system, special attention should also be paid to the way data stored on discarded storage equipment, such as magnetic storage devices and flash discs for smart mobile devices, notebooks, desktops and usb sticks. The simple erasure of files on these devices is considered inadequate to prevent data recovery, which is feasible by using simple and widely available artificial means. Another important issue is the person who asks for the erasure. It is quite difficult for a data controller/processor by himself/herself to take this decision without legal help.

In summary, it is worth noting that all technical approaches to safeguard the right to be forgotten are vulnerable to unauthorized creation of

[106] J. Zittrain., A History of Online Gatekeeping, Harvard Journal of Law and Technology, Vol. 19, No. 2, 2006

[107] P. Druschel, M. Backes, R. Tirtea, The right to be forgotten-between expectations and practice, European Network and Information Security Agency (ENISA) [2011], p.9 <https://www.enisa.europa.eu/publications/the-right-to-be-forgotten> accessed 30 December 2019

[108] Ibid. p. 10

copies, and disperse them when they expire. Thus, the right to be forgotten cannot be guaranteed by technical means alone. It is clear that a more complete solution will include legal requirements to make it practically difficult to find personal data that has expired.

15. CONCLUSIONS

In this Dissertation Thesis was examined the fundamental right to data protection and especially the right to erasure as a part of it. We also examine the concepts of the right to erasure, its material and personal scope, as well as, its relationship with other fundamental rights, in the light of General Data Protection Regulation and relevant decisions of the European Court of Justice. We also, examine time, which is an important element to be taken into account in balancing opposing interests.

The right to be forgotten, as it has been shaped till today, is certainly not complete and not clear. But it is a small step forward that contributes to data subject's protection.

An important problem to be understood is that any attempt to legislate in Europe reflects a specific political and legal compromise under the specific circumstances and within a specific social economic and technological context. It is true that the adoption of internet-related legislation faces significant difficulties, which have mentioned many times above: the speed of technological developments, the lack of speed of legislators, the nature of Internet are some of the problems. These problems need to be overcome with the co-operation of both legal and technological science.

However, 'legalization' of the right to be forgotten is now needed more than ever because Internet has become uncontrolled and individuals feel helpless. It is very important common practices (or even an international treaty someday) to be applied in all countries because the problem of protecting personal data on the Internet extends beyond the borders of the European Union. A legal regulatory framework is needed to ensure legal certainty in the management of personal data.

Article 17 of GDPR recognizes the right of data subjects to request for the erasure of their personal data provided there is a legal basis for doing so. However, the successful exercise of this right is not so clear. In order to do this, data subject must prove that: a) the inclusion of a particular search result associated with his/her name causes significant harm to his interests and b) that his/hers interests override those of the search engine.

In practice, it is really difficult to apply the right to erasure. Firstly, one needs to know if the right can be invoked in the first place. In case the answer is yes, secondly, one needs to evaluate how the right to erasure can be applied in a balanced way, considering all interests, rights and freedoms at stake.

GDPR installs a fair balancing framework that safeguards any fundamental rights and freedoms as they are affected by the processing of personal data. Courts are also oriented in this direction. But still there are several potential hurdles that might obstruct an effective exercise of the right to erasure. These may arise from legal measures safeguarding other fundamental rights, freedoms and interests.

It is obvious that the problems cannot be solved overnight, but a sound regulatory infrastructure is absolutely necessary to ensure both the protection of individuals and that the expansion of Information and Communications Technology (ICT) occurs in a manner that respects fundamental rights, freedoms and interests.

After all, should there be a right that make search engines erase information about individuals? Should there be a right to be forgotten? The answer is absolutely yes. But should search engines erase each and every information requested be data subjects? Sometimes the answer is yes and sometimes the answer is no. Each case is different and nobody could give an answer in advance.

Bibliography

Legislation and Prepatory Works

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (2000), OJ L8/1.

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, (2002) OJ L 201/37.

European Commission, 'Commission Staff Working Document Accompanying the document Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) {COM(2017) 10 final} <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0003> accessed 15 November 2019

European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century' (25 January 2012) COM(2012) 9 final.

European Commission, 'Impact Assessment Accompanying the Proposals for General Data Protection Regulation and Directive on Data Protection in Police and Judicial Matters' (Commission Staff working Paper, 25 January 2012) SEC(2012) 72 final.

European Data Protection Supervisor, Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit', [11 April 2017] <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf> accessed 08 December 2019

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014AP0212> accessed 18 December 2019.

Article 29 Working Party, 'Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites' (30 May 2002) WP 56

Article 29 Working Party, 'Opinion on the Use of Location Data with a View to Providing Value- Added Services' (November 2005) WP 115.

Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (20 June 2007) WP 136.

Article 29 Working Party, 'Working Document 1/2008 on the Protection of Children's Personal Data' (18 February 2008) WP 147.

Article 29 Working Party, 'Opinion 1/2008 on Data Protection Issues Related to Search Engines' (4 April 2008) WP 148.

Article 29 Working Party, 'Opinion 5/2009 on Online Social Networking' (12 June 2009) WP 136.

Article 29 Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (16 February 2010) WP 169.

Article 29 Working Party, 'Opinion 02/2010 on Online Behavioural Advertising' (22 June 2010) WP 171.

Article 29 Working Party, 'Opinion 13/2011 on Geolocation Services on Smart Mobile Devices' (16 May 2011) WP 185.

Article 29 Working Party, 'Opinion 15/2011 on the Definition of Consent' (13 July 2011) WP187.

Article 29 Working Party, 'Opinion 3/2012 on Developments in Biometric Technologies' (27 April 2012) WP 193.

Article 29 Working Party, 'Opinion 05/2012 on Cloud Computing' (1 July 2012) WP 196.

Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (02 April 2013) WP 203

Article 29 Working Party, 'Guidelines on Automated Decision-Making and Profiling for the purposes of Regulation 2016/679 (06 February 2018) WP251

Belgian Privacy Commission, Frequently Asked Questions - Google Street View, <https://www.dataprotectionauthority.be/faq-themes/the-internet/google-street-view> accessed 2 December 2019.

Data Protection Working Party, Opinion 4/2007 on the concept of personal data, <https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf> accessed 03 December 2019.

ENISA, The right to be forgotten-between expectations and practice (20 November 2012) <https://www.enisa.europa.eu/publications/the-right-to-be-forgotten> accessed 26 November 2019

European Commission, 'Building a European Data Economy' (10 January 2017) <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy> accessed 22 December 2019

European Data Protection Supervisor, 'Developing a 'toolkit' for Assessing the Necessity of Measures That Interfere with Fundamental Rights. Background paper' (16 June 2016) < <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Con

sult_ation/Papers/16-06-16_Necessity_paper_for_consultation_EN.pdf> accessed 28 December 2019.

European Union Agency for Fundamental Rights (FRA) and Council of Europe, Handbook on European Data Protection Law (Publications Office of the European Union, Luxembourg, 2018).

European Union Agency for Fundamental Rights (FRA), 'Opinion on the Proposed Data Protection Reform Package' (2012) FRA Opinion 2/2012.

OECD, 'The OECD Privacy Framework' (2013) <www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 9 May 2014.

Case Law

Court of Justice of the European Union

AffishBV v Rijksdienst voor de Keuring van Vee en Vlees [17 July 1997] Court of Justice of the European Union C-183/95.

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado [24 November 2011] Court of Justice of European Union Joined Cases C-468/10 and C-469/10

Coty Germany v Stadtsparkasse Magdeburg [16 April 2015] Court of Justice of the European Union C-580/13

Deutsche Telekom AG v Bundesrepublik Deutschland [5 May 2011] Court of Justice of the European Union C-543/09.

Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [13 May 2014] Court of Justice of the European Union C-131/12.

L'Oreal v eBay [12 July 2011] Court of Justice of the European Union C-324/09

Lindqvist v Aklagarkammaren i Jonkoping [6 November 2003] Court of Justice of the European Union C-101/01.

Markkinaporssi and Satamedia v. Finland [27 June 2017] Court of Justice of the European Union C-73-07

Maximillian Schrems v Data Protection Comissioner [06 October 2015] Court of Justice of the European Union C-362/2014

Maximilian Schrems v Facebook Ireland Limited [25 January 2018] Court of Justice of the European Union C-498/16.

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

Österreichischer Rundfunk and others [20 May 2003] Court of Justice of the European Union Joined Cases C-465/00, C-138/01 and C-139/01.

Patrick Breyer v Bundesrepublik Deutschland [19 October 2016] Court of Justice of the European Union C-582/14.

Promusicae v Telefónica [29 January 2008] Court of Justice of the European Union C-275/06.

SABAM v Netlog [16 February 2012] Court of Justice of the European Union C-360/10.

Scarlet Extended v Sabam [24 November 2011] Court of Justice of the European Union C70/10.

Spain and Finland v Parliament and Council [9 September 2004] Court of Justice of the European Union C-184/02.

Tietosuojavaltuutettu v Satakunnan Markkinapörssi & Satamedia [16 December 2008] Court of Justice of the European Union C-73/07.

Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [9 November 2010] Court of Justice of the European Union Joined Cases C-92/09 and C-93/09.

European Court of Human Rights

Couderc and Hachette Filipacchi Associés v France, [10 November 2015] European Court of Human Rights 40454/07.

Delfi AS v Estonia [16 June 2015], European Court of Human Rights, No 64569/09

Éditions Plon v France [18 May 2004] European Court of Human Rights 58148/00.

Editorial Board Of Pravoye Delo and Shtekel v Ukraine [05 April 2011], European Court of Human Rights 33014/05

Fuchsmann v Germany [19 October 2017] European Court of Human Rights 71233/13.

Handyside v The United Kingdom [07 December 1976] European Court of Human Rights [24,5393/72]

Neij and Sunde Kolmisoppi v Sweden (Pirate Bay Case) [19 February 2013] European Court of Human Rights 40397/12.

Österreichischer Rundfunk v Austria [7 December 2006] European Court of Human Rights 35841/02.

PETA Deutschland v Germany Case [2012], European Court of Human Rights, [No. 43481/09]

The Observer and the Guardian v The United Kingdom [26 November 1991] European Court of Human Rights 13585/88

Times Newspapers Ltd (Nos 1 and 2) v The United Kingdom [10 June 2009] European Court of Human Rights 3002/03 and 23676/03.

Timpul Info-Magazin and Anghel v. Moldova [02 June 2008], European Court of Human Rights 42864/05

Von Hannover v Germany [24 September 2004] European Court of Human Rights 59320/00.

Books

Bernal P (2014), Internet Privacy Rights: Rights to Protect Autonomy, Cambridge University Press, Cambridge.

Corrales M., Fenwick M. and Forgo N., (2017) New Technology, Big Data and the Law, Springer Nature Singapore

Inglezakis I. (2014), The right to oblivion and its limitations, Sakkoulas Publications, Athens.

Klang M. and Murray A. (2005), Human rights in the digital age, London; Portland, Or.: Glasshouse Press: Routledge-Cavendish.

Mayer-Schoenberger V. (2009), Delete the Virtue of Forgetting in the Digital Age, Princeton University Press

Peers S., Hervey T., Kenner J. and Ward A. (2014), The EU charter of fundamental rights: a commentary, Hart Publishing <https://www.bloomsburycollections.com/book/the-eu-charter-of-fundamental-rights-a-commentary/> accessed 20 December 2019

Rucker D. and Kugler T, (ed.) (2017), New European General Data Protection Regulation: A Practitioner's Guide, Hart Publishing, UK.

Articles

Accenture Strategy και Oxford Economics, Digital Disruption: the Growth Multiplier (2016), <https://www.accenture.com/us-en/insight-digital-disruption-growthmultiplier.asp> accessed 15 November 2019

Ambrose M. and Ausloos D, The right to be Forgotten across the Pond, JOURNAL OF INFORMATION POLICY 3 (2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2032325> accessed 26 November 2019

Ambrose M. and Aulsloos J., Timing the Right to be Forgotten, A Study into 'time' as a factor in deciding about retention or erasure of data [2015], < http://archive.ceu.hu/publications/korenhof/2015/43831> accessed 11 December 2019

Angelopoulos C and others, 'Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation' (IviR, 2015)< <https://pure.uva.nl/ws/files/8763808/IVIR_Study_Online_enforcement_through_self_regul ation.pdf> accessed 15 October 2019.

Ausloos J, 'Google v Spain at the Court of Justice of the EU' (Tech, Policy & Society blog, 5 March 2013) <https://jefausloos.wordpress.com/2013/03/05/google-v-spain-at-theeuropean-court-of-justice> accessed 25 November 2019.

Ausloos J, 'The Interaction between the Rights to Object and to Erasure in the GDPR' (CITIP blog, 25 August 2016) <www.law.kuleuven.be/citip/blog/gdpr-update-the-interactionbetween-the-right-to-object-and-the-right-to-erasure> accessed 22 November 2019.

Brown I, 'The Economics of Privacy, Data Protection and Surveillance' (2013) <http://papers.ssrn.com/abstract=2358392> accessed 18 October 2019.

Danezis G and others, 'Privacy and Data Protection by Design – from Policy to Engineering' (ENISA, December 2014) <www.enisa.europa.eu/publications/privacy-and-data-protectionby-design> accessed 15 October 2019.

De Andrade N.N.G., Oblivion: The right to Be different….. from Oneself Reproposing the Right to be Forgotten, European University Institute - Law Department; UC Berkeley Law School, Berkeley Center for Law & Technology, (2012) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033155> accessed 28 November 2019

Della Morte G., International Law between the Duty of Memory and the right to Oblivion, [2014 International Criminal Law Review 14], <https://heinonline.org/HOL/Page?public=true&handle=hein.journals/intcrimlrb14&div=26&start_page=427&collection=journals&set_as_cursor=0&men_tab=srchresults> accessed 18 December 2019

Gliszezynska-Grabiaw A., Memory Laws or Memory Loss? Europe in search of its Historical Identity Through the National and Internationa Law, [34 Polish Y.B. Int'L, 2014] <https://heinonline.org/HOL/Page?public=true&handle=hein.intyb/polyeai0034&div=10&start_page=161&collection=intyb&set_as_cursor=4&men_tab=srchresults> accessed 31 December 2019

Hemminki S., Nurmi P. and Tarkoma S., Accelerometer-Based Transportation Mode Detection on Smartphones [ACM Press 2013] <http://dl.acm.org/citation.cfm?doid=2517351.2517367> accessed 02 December 2019

Inglezakis I., The Right to Forget: A New Digital Right for Cyberspace, II.C (2018), <https://www.lawspot.gr/nomika-blogs/ioannis_igglezakis/dikaioma-sti-lithi-ena-neo-psifiako-dikaioma-gia-ton-kyvernohoro> accessed 26 November 2019

Kate A.M., (Re)Difing Public Officials and Public Figures: A Washington State Primer.(Archive) *Seattle University Law Review*. Seattle University School of Law. Vol 23:1155-2000. <https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1646&context=sulr> accessed 12 December 2019

Kelly M.J; David S., The Right to Be Forgotten, 2017 U. Ill. L. Rev. 1 (2017)

<https://heinonline.org/HOL/LuceneSearch?terms=Michael+J.+Kelly%3B+Satolam+David%2C+The+Right+to+Be+Forgotten%2C+2017+U.+Ill.+L.+Rev.+1++%282017%29&collection=all&searchtype=advanced&typea=text&tabfrom=&submit=Go&all=true>accessed 03 December 2019

Koops B-J., Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice. [Tilburg Law School Legal Studies Research Paper Series, No. 08/2012], 2 <http://ssrn.com/abstract=1986719> accessed 23 November 2019

Korenhof P and others, 'Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data' in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), Reforming European Data Protection Law, vol 20 (Springer, Dordrecht, 2015) 171.

Kuczerawy A and Ausloos J, 'NoC Online Intermediaries Case Studies Series: European Union and Google Spain' (2015) <http://ssrn.com/abstract=2567183> accessed 22 September 2019

La Rue F., Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Meeting of the Security Council in Arria format on:«Protecting journalists» (2013) <https://www.ohchr.org/Documents/HRBodies/SP/StatementSRFreedexProtectingJournalists13Dec2013.pdf> accessed 11 December 2019.

Mitrou L and Karyda M. 'EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?' Corfu, Greece, 2012. <http://papers.ssrn.com/abstract=2165245> accessed 28 November 2019

Lazaroiu G., The Growth of Networked Media, 1 Contemp. Readings L. & Soc. Just. 146 (2009) <https://heinonline.org/HOL/Page?public=true&handle=hein.journals/conreadlsj1&div=29&start_page=146&collection=journals&set_as_cursor=0&men_tab=srchresults> accessed 02 December 2019

Rosen J, The Web Means the End of Forgetting, New York Times, June 2010, <http://www.nytimes.com/2010/07/25/magazine/25privacyt2.html?pagewanted=all&_r=0> accessed 23 November 2019.

Tamp A. and George D., Oblivion, Erasure and Forgetting in the Digital Age, JIPITEC 5 (2) (2014) < https://www.jipitec.eu/issues/jipitec-5-2-2014/3997> accessed 28 November 2019

Temperton J., EU Demands 'Right to be Forgotten' be Applied Globally, [WIRED Nov. 26, 2014], <http://www.wired.co.uk/news/archive/2014-11/26/eu-right-to-beforgotten-extended> accessed 25 November 2019.

Van Calster G and others, 'Not Just One, but Many "Rights to Be Forgotten" (15 May 2018) 7(2) Internet Policy Review <https://policyreview.info/articles/analysis/not-just-one-manyrights-be-forgotten> accessed 02 November 2019

Weber R., The Right to Be Forgotten: More Than a Pandora's Box?, JIPITEC 2011 (2), 120 (2011) <https://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf> accessed 26 November 2019

Wechsler S., The Right to Remember: The European Convention on Human Rights and the Right to Be Forgotten, [49 Colum. J.L.&Soc.Probs. 135,2015] <https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/collsp49&id=142&men_tab=srchresults> accessed 25 November 2019

Zheng N, Paloski A and Wang H, 'An Efficient User Verification System via Mouse Movements', Proceedings of the 18th ACM conference on Computer and communications security (ACM 2011) <http://dl.acm.org/citation.cfm?id=2046725> accessed 12 November 2019

Zittrain J., A History of Online Gatekeeping, Harvard Journal of Law and Technology, Vol. 19, No. 2, 2006