*Bachelor of Law*
Bachelor's final dissertation (21067/22747)
Academic year 2016-2017

# THE RIGHT TO BE FORGOTTEN:
## A DESCRIPTIVE OVERVIEW OF THE RIGHT TO BE FORGOTTEN

Juan Estheiman Amaya Camposeco

NIA: 165229

Final dissertation tutor:

Marisa Iglesias Vila

**DECLARACIÓ D'AUTORIA I ORIGINALITAT**

Jo, *Juan Estheiman Amaya Camposeco*, certifico que el present treball no ha estat presentat per a l'avaluació de cap altra assignatura, ja sigui en part o en la seva totalitat. Certifico també que el seu contingut és original i que en sóc l'únic autor, no incloent cap material anteriorment publicat o escrit per altres persones llevat d'aquells casos indicats al llarg del text.

Juan Estheiman Amaya Camposeco
Barcelona, 2 de Juny de 2017

# ABSTRACT

On the 5th of March 2010, Mr Costeja González lodged a complaint in the Spanish Data Protection Agency (AEPD) against the publisher of the Spanish newspaper La Vanguardia, Google Spain and Google Inc. In his complaint, he requested that personal data related to him be removed or concealed. The case, known as *Google v. Costeja*, reached the Court of Justice of the European Union (CJEU) with a request for a preliminary ruling. On the 9th of May 2014, the CJEU recognised that a "right to be forgotten" was rooted in the provisions of Directive 95/46 (the Data Protection Directive).

This final dissertation aims to present a general overview of a "right to be forgotten". Through a descriptive approach, it intends to provide an outline of the background, present and future of a "right to be forgotten". A special emphasis is made on the balancing of interests underlying such a right, which are closely linked to the right to privacy, the right to freedom of expression and access to information, and the principle of rehabilitation. Furthermore, this final dissertation hopes to provide an insightful analysis of Google v. Costeja, Google's implementation of a "right to be forgotten" and the recent and future developments on such right.

We conclude that the CJEU was correct in recognising a "right to be forgotten" within EU law. However, it is necessary to acknowledge that such a right actually encompasses different "rights to be forgotten". Lastly, we call for the need of a hybrid system in the implementation of the "rights to be forgotten" by private companies.

# INDEX

## Abbreviations

- Charter of Fundamental Rights of the European Union (CFREU)
- Court of Justice of the European Union (CJEU)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/45 or "the Directive")
- European Court of Human Rights (ECHR)
- European Union (EU)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation / GDPR)
- Right to be delisted (RTBD)
- Right to be forgotten (RTBF)

## Definitions

- '**data subject**': an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; in other words, a "an individual or natural person"[1].
- '**personal data**': any information relating to an identified or identifiable natural person[2].
- '**processing**': any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[3];
- '**controller**': 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law[4];
- '**information society service**': any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services[5].

---

[1] Directive 95/46 (Data Protection Directive) Article 2. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[2] *Id. supra.*
[3] *Id. supra.*
[4] *Id. supra.*
[5] *Id. supra.*

# INTRODUCTION

*"It's because of data permanence that we think twice before posting a photo, or check that a connection is secure before entering a password, or ponder whether an offhand comment on a message board might raise the eyebrows of a would-be employer in twenty years. Who would have guessed that parents need to talk about all of this with their children, all of the issues related to preserving privacy and security online, before they even have the first conversation about sex? Yet this is the world we live in, in which data cannot be put back in the box."*[6]

Google's Eric Schmidt and Jared Cohen, Founders of Google.

The protection of personal data remains an important concern for citizens. According to a Eurobarometer published by the European Commission in 2015 on data protection[7], over seven out of ten people (71%) agree that providing personal information is increasingly part of modern life, while two-thirds of the respondents (67%) said that they are worried about having no control over the information they provide online, and only 15% feel they have complete control.

There have been significant technological advancement and progress since the mid-1990s, when the EU first adopted a set of rules that defined how personal data should be protected. Today, the way in which data is collected, processed and accessed no longer resembles the methods that were used around two decades ago. In addition to changing the ways we communicate, relate and behave, this evolution in technology has also entailed an evolution in the interpretation of fundamental rights, such as the right to privacy. It is in the context of the digital age that the Right to Be Forgotten (RTBF) appears, and with it, the debate around its meaning, scope, implementation, and relation with other rights.

At the core of the debate on the RTBF lie fundamental discussions such as the debate on Privacy v. Freedom of Expression[8], the power of Internet companies' control of data over individuals' in the "data economy" age[9], or even the extent of the right to self-determination, as it could express "the ability to reinvent oneself, to have a second chance to start-over and present a renewed identity to the world"[10].

The objective of this final dissertation is to present a general overview of the RTBF. In doing so, this dissertation takes a predominantly descriptive approach by mostly compiling authors' research on the RTBF. By taking a general and descriptive approach, rather than a more

---

[6] (ERIC SCHMIDT & JARED COHEN, 2014)
[7] (EUROPEAN COMMISSION, 2015)
[8] (ROSEN, 2012, p. 90)
[9] (THE ECONOMIST - Leaders Section, 2017) Leaders Section. Regulating the internet giants: The world's most valuable resource is no longer oil, but data. The Economist (May 6th 2017) http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource
[10] (IGLEZAKIS, 2016) quoting Andrade, N. G. de, Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization, in: S. Gutwirth et al (eds), Privacy and Data Protection. An Element of Choice (2011), pp. 65-97.

technical one, this dissertation hopes to make the topic accessible to any reader. Given the general relevance of the topic, this dissertation also hopes to provide any reader with a necessary overview of the background, present and future of the RTBF so that they are capable of questioning and reaching their own conclusions on the matter.

To fulfil its objectives, this dissertation has been structured in the following three main sections:

1. The first section provides an overview of the background to the RTBF, with which we hope to contextualise the topic. This first section is divided in three subsections. The first subsection presents a history of the evolution of the right to privacy and briefly elaborates on how the digital age has changed the conceptions of privacy. The second subsection is of key importance given that it examines the fundamental interests at stake behind the RTBF. We have identified such interests to be internet privacy, public interest and the value of forgetting. The third subsection aims at providing the reader with a set of questions so that he or she can begin to critically assess the rest of the dissertation.
2. The second section presents the most important case on the RTBF within the EU: *Google v. Costeja* (2014). If a reader has heard of the RTBF, it is almost certainly because of this case. The relevance of the case stems from the Court of Justice of the European Union (CJEU) recognising that a RTBF was rooted in the provisions of Directive 95/46[11]. In this section, we will analyse the facts underlying the CJEU's decision and we will present the most important critiques and comments on the decision.
3. The third section hopes to build on the general notions of what the reader has been presented by that point. The first subsection will present a conceptual analysis of the "right" or "rights" to be forgotten. With this, we will assess how the RTBF is actually more of a spectrum of rights, rather than just one only right. In the second subsection, we will consider Google's practical implementation of the RTBF and a data-based study on what is "being forgotten". Finally, in the third subsection we will portray the developments on the RTBF since the CJEU's decision. With those three subsections, we hope the reader will have a clear overview of the *état de la question* regarding the RTBF.

This dissertation also includes an annex which is divided into two main sections. The first one comprises relevant legislation that we will be recurrently referencing throughout the dissertation. The second annex provides a summary of the full Google v. Costeja preliminary ruling. For the sake of accessibility and conciseness, we decided to move the summary of the preliminary ruling to the annexes. However, by including it, we still hope to give readers the opportunity of expanding on Google v. Costeja, in case they might wish to so.

Lastly, we would like to make some clarifications on the use of certain terminology throughout the dissertation. As we will see, the RTBF actually comprises different "rights to

[11] (IGLEZAKIS, 2016, p. 4)

be forgotten"[12]. Given that this idea is relatively recent, when some authors talk about the RTBF, they might be referring to one of the "rights to be forgotten" in particular. This is especially the case when discussing the "right to be delisted"[13]. Furthermore, throughout this dissertation, when is not clear which particular "right to be forgotten" is to be referenced, we also refer to it as "a RTBF".

[12] In section 3.1. of this dissertation.

[13] This was the right recognised by the CJEU in Google v. Costeja. For more, see section 3.1.3. of this dissertation.

# CONTENT

## 1. BACKGROUND OF THE RIGHT TO BE FORGOTTEN (RTBF)

### 1.1. The evolution of privacy and the RTBF

In 1890, Samuel Warren and Louis Brandeis were the first to systematically describe a legal right to privacy[14]. They defined it as a right to essentially protect one's "inviolate personality" from intrusion or unwanted revelation[15]. In essence, they called for a "right to be left alone"[16]. Traditionally, privacy interests were implicit in legal or social protection of personal property and space, intimate settings, or personal effects[17]. However, the modern evolution of the right to privacy is closely tied to the industrial-age technological development, ranging from telephones or cameras, to flying machines[18], which have allowed new intrusions into intimate aspects of life[19]. In return, the law has reacted to protect the sphere of the private[20]. Thus, digital technology-computing, databases, the Internet, mobile communications, etc. call for further evolution of privacy rights, both conceptually and in law[21].

In the analogue age, public records such as bankruptcy filings or criminal proceedings were all available, but remained "in practical obscurity in courthouse basements or isolated file cabinets"[22]. The records were difficult to locate or assemble into a useful dossier[23]. The digital age has changed how we now access and organise data[24]. Government records are now stored digitally, and often linked to the Internet or other networks[25]. In this context, Jerry Berman[26] and Deirdre Mulligan[27] note three major digital developments that deeply affect privacy[28]:

---

[14] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 286)
[15] (WARREN, Samuel D. & BRANDEIS, Louis D., 1890, p. 205)
[16] *Id. supra.*
[17] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 284)
[18] *Id. supra.*
[19] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 284) quoting Dermis F. Hemandez, Litigating the Right to Privacy: A Survey of Current Issues, 446 PLIIPAT 425, 429 (1996).
[20] *Id. supra.*
[21] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 284)
[22] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 301) quoting DOJ v. Reporters Cornm. for Freedom of the Press, 489 U.S. 749, 762 (1989).
[23] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 301) quoting Matthew D. Bunker et. al., Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology, 20 FLA. ST. U.L. REY. 543, 583 (1993).
[24] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 301)
[25] *Id. supra.*
[26] Jerry Berman is the founder of the Center for Democracy and Technology (CDT). CDT is a Washington, DC based Internet public policy organization. CDT plays a leading role in free speech, privacy, Internet Governance and architecture issues affecting democracy and civil liberties on the global Internet.
[27] Deirdre Mulligan is Staff Counsel at the Center for Democracy and Technology, a public interest organization dedicated to developing and implementing public policies designed to protect and enhance civil liberties and democratic values in the new digital media. Center for Democracy & Technology <http://www.edt.org>.
[28] (BERMAN, J. & MULLIGAN, D., 1999, págs. 554-555)

> "1. the increase in data creation and the resulting collection of vast amounts of personal data, caused by the recording of almost every modern interaction;
> 2. the globalization of the data market and the ability of anyone to collate and examine this data; and
> 3. lack of the types of control mechanisms for digital data that existed to protect analogue data."

As DeVries argues, these three developments "all concern the changes wrought by digital technology on the ability to manipulate information"[29]. In particular, he states that, "individuals have little ability to control this collection or manipulation"[30].

The RTBF appears in the context of giving back control to individuals of the access to information about them. The first expression of the RTBF was linked to the principle of rehabilitation in the context of criminal sentences[31]. Such right was based on the core idea of limiting public interest to certain information about oneself. This "RTBF" then also expanded to the context of insolvency proceedings[32]. Throughout the 20th century, many countries adopted legislation which enshrines the RTBF in the context of past criminal offenses[33].

In the context of digital technologies, France was a pioneer in setting a RTBF with its 1978 Data Protection Act[34]. In the European Union, the current framework[35] for data protection is Directive 95/46, which was adopted in 1995[36]. On the 13th of May 2014, the CJEU issued a decision on May 13, 2014, known as Google v Costeja, in which it found that the RTBF is rooted in the provisions of Directive 95/46[37]. However, it is important to point out, in the words of former EU Commissioner for Justice Viviane Reding, that "this right builds on already existing rules" [38], and is not an *ex novo* right[39]; "although the judgment was only handed down by the court recently, this decision has been taken in 1995, when the European law which protects individuals' data was drafted"[40].

However, the Directive will soon be replaced with the General Data Protection Regulation (GDPR), which will enter into force in May 2018[41]. In contrast to the Directive, the GDPR now expressly recognises a RTBF in its Article 17[42].

---

[29] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 291)
[30] (DeVRIES, Protecting Privacy in the Digital Age,, 2003, p. 292)
[31] (W. G. VOSS & C. C. RENARD, 2016, p. 299)
[32] (W. G. VOSS & C. C. RENARD, 2016, p. 338)
[33] (W. G. VOSS & C. C. RENARD, 2016, p. 338)
[34] (W. G. VOSS & C. C. RENARD, 2016, p. 285)
[35] (SCHWARTZ, P. & SOLOVE, D., 2014, pág. 881)
[36] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[37] (IGLEZAKIS, 2016, p. 4)
[38] (REDING, 2012) http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm
[39] (IGLEZAKIS, 2016, p. 4)
[40] (REDING, 2012) http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm
[41] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

## 1.2. Interests at stake in the RTBF

As we will see, Google v Costeja was essential in recognising a RTBF in the context of data protection. However, before proceeding to analyse the case it is important to highlight the main fundamental conflicts behind a RTBF. It should be noted that there are different conceptual approaches about this new right in the literature[43]. Behind the RTBF most authors generally see a conflict between the right to privacy and the right to freedom of expression[44]. In this section, we will focus on specifying the scope of such rights regarding the RTBF. Finally, we will also briefly elaborate on what we identified as another very important conflict underlying the RTBF: the potential value of forgetting.

### 1.2.1. Internet privacy

In a report by the European Union Committee of the House of Lords of the United Kingdom on Google v. Costeja, the authors labelled the RTBF as constituting "a right to censorship of the internet"[45]. While such claims are excessive, as I will argue later, they are important to clearly portray the extent of the privacy v. freedom of expression conflict behind the RTBF.

The RTFB is fundamentally based on the rights to respect for private and family life and the protection of personal data, enshrined in arts. 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU)[46]. While these rights are generally seen as falling under the broader category of the "right to privacy", it is important to distinguish this fundamental right from the more precise concept of *internet privacy*. In defining internet privacy, we will particularly focus on Cécile de Terwangne's paper: "Internet Privacy and the Right to Be Forgotten/Right to Oblivion".

When considering internet privacy, De Terwangne warns us that *privacy* is not to be read as *intimacy* or *secrecy*[47]. It rather refers to another dimension of privacy, i.e. individual autonomy, the capacity to make choices, to make informed decisions, etc. In other words, "to keep control over different aspects of one's life"[48]. In the context of the internet, this dimension of privacy means informational autonomy or informational self-determination[49]. Information self-determination means the control over one's personal information, the

---

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[42] In Annex 1.3. of this dissertation.

[43] (IGLEZAKIS, 2016, p. 3)

[44] Amongst others: (ROSEN, 2012), (HUSOVEC, 2014), (ARTICLE 19, 2014)

[45] (European Union Committee, HOUSE OF LORDS OF THE UNITED KINGDOM, 2014, p. 15) paragraph 35.

[46] In Annex 1.2. of this dissertation.

[47] (DE TERWANGNE, 2012, p. 110)

[48] *Id. supra.*

[49] *Id. supra.*

individual's right to decide which information about themselves will be disclosed, to whom and for what purpose[50]. In this regard, internet has entailed two main difficulties[51]:

- Control over who you are disclosing your information to: this is especially relevant in the context of search engines' activities, as they make data accessible to virtually anyone[52].
- The moment when disclosure occurs: what you have disclosed at one stage in your life you do not necessarily want to be permanently available.

As we will see later, both Google v. Costeja and the Manni case elaborate on these ideas when justifying and setting the scope for the RTBF.

### 1.2.2. Public interest

Given the fundamentally different conceptions and importance of the right to freedom of expression between the US and Europe[53], the RTFB has been especially criticised amongst US authors. Some of their concerns are based on the idea that this right will have chilling effects on free expression, as it might force Internet intermediaries to censor the contents that they publish or to which they link, and hence, lose their neutral status[54]. Others also argue that the RTBF would hamper everyone interested in finding out inconvenient truths about those who would like their past covered up[55].

Freedom of expression and the freedom to receive information are enshrined in art. 11 of the CFREU[56], which proclaims that everyone has the right to freedom of expression and that right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers[57]. Furthermore, art. 11 also proclaims that the freedom and pluralism of the media shall be respected.

For this section, we will echo the view of the Organisation ARTICLE 19[58] on the right to freedom of expression in the context of the RTBF. I interpret such views as emphasising the importance of the public's legitimate interest in certain information, within the broader value of freedom of expression. I see this as an important clarification. As it currently stands, after the cases that we will study, the RTBF does not affect the possibility for unwanted information to exist, but rather that such information is less easily accessible by different

[50] *Id. supra.*
[51] (DE TERWANGNE, 2012, p. 111)
[52] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraphs 36-38.
[53] (SCHWARTZ, P. & SOLOVE, D., 2014, pág. 877)
[54] (IGLEZAKIS, 2016) quoting (ROSEN, 2012)
[55] (THE ECONOMIST, 2014)
[56] In Annex 1.1 of this dissertation.
[57] Charter of Fundamental Rights of the European Union. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[58] ARTICLE 19 is an international human rights organisation, founded in 1987, which defends and promotes freedom of expression and freedom of information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information.

means (e.g. delisting links or obscuring access to certain information)[59]. However, it is true that within academia some privacy advocates also call for stronger variations of the RTBF which would effectively delete data after certain conditions are met[60].

According to ARTICLE 19, the public interest is a concept which must be interpreted broadly to encompass "important information of public concern"[61]. This includes, but is not limited to, politics, public health and safety, law enforcement and the administration of justice, consumer and social interests, the environment, economic issues, the exercises of power, and art and culture[62].

In this regard, ARTICLE 19 clarifies that public interest "does not include purely private matters in which the interest of members of the public, if any, is merely salacious or sensational"[63]. In particular, they refer to the ECHR's criteria of putting a higher value on information which would contribute to public debate, rather than a lesser interest in merely providing to the public curiosity[64].

At the same time, they also recognise that public figures, especially leaders of states and elected representatives, have a lesser expectation of privacy than private figures or even lesser officials[65]. The more significant a public figure is, the more they should be subject to, and tolerant of, the highest levels of scrutiny in accordance with the principles of democratic pluralism[66]. In connection to this, they reference the Council of Europe's view that certain facts relating to the private lives of public figures, particularly politicians, may indeed be of interest to citizens, and it may therefore be legitimate for readers, who are also voters, to be informed of those facts[67]. Critics of Google v Costeja argue that this may also be the case when past events are relevant in the performance of other duties of public nature, such as those of teachers[68] or doctors[69].

As we will elaborate on later[70], one of the most controversial decisions of Google v. Costeja was the general prevalence set by the CJEU of the rights to private life and protection of data privacy over the right to freedom of expression[71]. Another very criticised point of the preliminary ruling was the vagueness in its definition of public interest.

---

[59] In section 3.1. of this dissertation.
[60] In sections 3.1.5. and 3.1.6. of this dissertation.
[61] (ARTICLE 19, 2014, pág. 6)
[62] *Id. supra.*
[63] ARTICLE 19, Defining Defamation: Principles on Freedom of Expression and Protection of Reputation, July 2000.
[64] See Von Hannover no. 2 v Germany, nos. 40660/08 and 60641/08, [GC], 7 February 2012, at paragraph 110.
[65] (ARTICLE 19, 2014, pág. 6)
[66] Lingens v. Austria, No. 9815/82, 8 July 1986
[67] Resolution no 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy
[68] (HUSOVEC, 2014)
[69] (ECHIKSON, 2013)
[70] In section 2.4.3.1. of this dissertation.
[71] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 97.

### 1.2.3. The value of forgetting

*"Without forgetting it is quite impossible to live at all."* [72] Friedrich Nietzsche.

For Viktor Mayer-Schönberger, professor of internet governance at the Oxford Internet Institute of the University of Oxford, the RTFB "is not just about the legal, moral and technical arguments – but about what it is to be human"[73]. He holds that humans need to make decisions about the present and the future[74], and that forgetting enables us to think in the present, which is something necessary to help us make decisions[75]". He elaborates that "our brains reconstruct the past based on our present values". By doing this, he says that we constantly reconstruct ourselves, rather than stagnating in our pasts[76]. Mayer-Schönberger's views on the RTBF are connected with Andrade's stance that the RTBF is connected with the right to personal identity, insofar as it expresses "the ability to reinvent oneself, to have a second chance to start over and present a renewed identity to the world"[77].

As Husovec has pointed out, there can be "many instances when we want to give a second chance to people and relieve them from their personal history"[78]. In this regard, spent convictions for rehabilitated offenders, juvenile indiscretions or personal bankruptcies all share the same justification: a need to give people a second chance[79].

This could raise an interesting ethical question for the data age: "should the Internet be re-wired to be more like the human brain?[80]" From a more pragmatic perspective, however, Peter Fleischer, Google's Global Privacy Counsel, reminds us that "computers don't work that way"[81]. However, as we will see, different variations of the RTBF could actually resemble some of the forgetting mechanisms of the human brain[82].

## 1.3. Final questions to contextualise the discussion over the RTBF

Before proceeding to analyse Google v. Costeja, I would like to echo some of Google's Global Privacy Counsel Peter Fleischer's reflexions over "oblivion in the digital age"[83], for us to contextualise the RTBF and to have a more critical read of the CJEU's decision:

"1. If I post something online, should I have the right to delete it?

---

[72] Friedrich Nietzsche, On The Advantage And Disadvantage Of History For Life (1874).
[73] (MAYER-SCHÖNBERGER, 2013)
[74] *Id. supra.*
[75] *Id. supra.*
[76] *Id. supra.*
[77] Andrade, N. G. de, Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization, in: S. Gutwirth et al (eds), Privacy and Data Protection. An Element of Choice (2011), pp. 65-97.
[78] (HUSOVEC, 2014)
[79] *Id. supra.*
[80] (PETER FLEISCHER, 2011)
[81] *Id. supra.*
[82] In sections 3.1.4. and 3.1.5. of this dissertation.
[83] (PETER FLEISCHER, 2011)

2. If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it? Clearly, I should be able to ask the person who re-posted my picture to take it down. But if they refuse, or just don't respond, or are not find-able, what can I do?
3. If someone else posts something about me, should I have a right to delete it? This raises difficult issues of conflict between freedom of expression and privacy. Traditional law has mechanisms, like defamation and libel law, to allow a person to seek redress against someone who publishes untrue information about him. Granted, the mechanisms are time-consuming and expensive, but the legal standards are long-standing and reasonably clear. But a privacy claim is not based on untruth.
4. The Internet platforms that are used to host and transmit information all collect traces, some of which are Personally Identifiable Information (PII), or partially PII. Should such platforms be under an obligation to delete or anonymize those traces after a certain period of time? and if so, after how long? and for what reasons can such traces be retained and processed?
5. Should the Internet just learn to "forget"? Quite apart from the topics above, should content on the Internet just auto-expire? e.g., should all user posts to social networking be programmed to auto-expire? Or alternatively, to give users the right to use auto-expire settings? Is this actually feasible from a technical perspective?
6. Who should decide what should be remembered or forgotten? For example, if German courts decide German murderers should be able to delete all references to their convictions after a certain period of time, would this German standard apply to the Web? Would it apply only to content that was new on the Web, or also to historical archives? and if it only applied to Germany, or say the .de domain, would it have any practical impact at all, since the same content would continue to exist and be findable by anyone from anywhere?"

## 2. GOOGLE V. COSTEJA

Google v. Costeja is, to this date, the most important case on the RTBF in the EU. As mentioned previously, the CJEU's preliminary ruling declared the existence of a RTBF within the provisions of Directive 95/46, rather than created an *ex novo* right[84]. This distinction is important, given that, to our understanding, the CJEU's preliminary ruling proclaims a right resulting from "a reasonable reflection of the text of the Directive and the values embodied in it" [85], rather than altogether creating a new right. In this section, we will look into the facts of the case, the CJEU's decision and we will analyse the most important set of critiques to the decision.

[84] (IGLEZAKIS, 2016, p. 4)
[85] (HARVARD LAW REVIEW, 2014, p. 735)

## 2.1. The facts

On the 5th of March 2010, Mr Costeja González (a Spanish national), lodged a complaint in the Spanish Data Protection Agency (AEPD) against La Vanguardia Ediciones SL (the publisher of the Spanish newspaper La Vanguardia), Google Spain and Google Inc.

When entering Mr Costeja González's name in the Google group's search engine (Google Search), the results showed links to two pages from La Vanguardia newspaper from the 19th of January and the 9th of March 1998, which included the announcement of a foreclosure auction of Mr Costeja's home for the recovery of debts with the Spanish Social Security. According to Mr. Costeja, the foreclosure proceedings against him had already been resolved several years before he presented the complaint[86].

### 2.1.1. Mr. Costeja's complaint before the AEPD and the AEPD's decision

In Mr Costeja González's complaint, he requested[87]:

1. That La Vanguardia be required to either remove those pages or to alter any references to his personal data in the pages, so that it no longer appeared.
2. That Google Spain or Google Inc. be required to *remove or conceal* the personal data related to him, excluding it from the search results so that it no longer appeared in the links to La Vanguardia.

On the 30th of July 2010, the AEPD's decision on Mr. Costeja Gonzalez's complaint[88]:

1. Rejected his request regarding La Vanguardia. The AEPD argued that the inclusion of Mr. Costeja's information was legally justified, by the Ministry of Labour and Social Affairs objective of giving maximum publicity to the auction, to secure as many bidders as possible.
2. Upheld his request against Google Spain and Google Inc. The AEPD considered that:
    a. when the processing of personal data can compromise the fundamental right to data protection and the dignity of persons in the broad sense, the AEPD has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines.
    b. the obligation to withdraw the data or to prohibit access may be owed directly by the operators of search engines, without it being necessary to erase the data or information from the website where they appear.

### 2.1.2. Google Spain and Google Inc.'s claim against the AEPD's decision

[86] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph. 15.
[87] *Id. supra.*
[88] *Id. supra* paragraphs 16-17.

Google Spain and Google Inc. brought actions against the AEPD's decision before the Audiencia Nacional (Spanish National High Court). The Audiencia Nacional then stated that the actions raised the main question of the obligations that operators of search engines have in protecting the personal data of persons who do not want such data to be published. Given that the answer to the main question depended on the interpretation of Directive 95/46, the Audiencia Nacional decided to suspend the proceedings and to refer a series of questions to the CJEU for a preliminary ruling.

It is important to mention that formally, the applicable law to the case was the Spanish data protection law, the Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal[89]. Google's appeal, however, focused on the greater principles contained in the Data Protection Directive[90]. In particular, the company argued that its activity as a search engine fell outside of the Directive's personal and material scope and that any request for removal had instead to be addressed to the original publisher, in this case the La Vanguardia newspaper[91]. In addition, it contended that, being a US based corporation performing data processing operations there, the Directive could not apply, geographically speaking, to its activity[92]. Finally, it asserted that, while the principles of the Directive grant a general right to erasure of unlawfully processed personal data, they do not imply the right to request the removal of search results linking to harmful, embarrassing, and outdated, but lawful, protected, and available, material[93].

### 2.1.3. The Audiencia Nacional's questions to the CJEU

The Audiencia Nacional referred three main set of questions[94] to the CJUE regarding:

1. The territorial scope of application of EU data protection rules.
2. The issues relating to the legal position of an internet search engine service provider in the light of the Directive, especially in terms of its material scope of application.
3. The so-called RTBF and the issue of whether data subjects can request that some or all search results concerning them are no longer accessible through search engine[95].

## 2.2. The CJEU preliminary ruling on the "right to be forgotten"

On the 13th of May 2014, the CJEU issued its preliminary ruling. The CJEU's answer[96] to the questions referred to by the Audiencia Nacional was:

[89] (REYMOND, 2016, p. 6)
[90] *Id. supra.*
[91] *Id. supra.*
[92] *Id. supra.*
[93] *Id. supra.*
[94] Original questions in Annex 2.1. of this dissertation.
[95] (KELLY, 2015) paragraph 12.
[96] (EUROPEAN COMMISSION, 2014). European Commission. Factsheet on ECJ's ruling on the 'right to be forgotten' in relation to online search engines. Factsheet on the "Right to be Forgotten" ruling (C-131/12): http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

"1. On the territoriality of EU rules: Even if the physical server of a company processing data is located outside Europe, EU rules apply to search engine operators if they have a branch or a subsidiary in a Member State which promotes the selling of advertising space offered by the search engine;
2. On the applicability of EU data protection rules to a search engine: Search engines are controllers of personal data. Google can therefore not escape its responsibilities before European law when handling personal data by saying it is a search engine. EU data protection law applies and so does the right to be forgotten.
3. On the "Right to be Forgotten": Individuals have the right - under certain conditions - to ask search engines directly to remove links with personal information about them. This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing[97]. The court found that in this particular case the interference with a person's right to data protection could not be justified merely by the economic interest of the search engine. At the same time, the Court explicitly clarified that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media[98]. A case-by-case assessment is needed considering the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information. The role the person requesting the deletion plays in public life might also be relevant."

### 2.2.1. The Article 29 Working Group's guidelines on the implementation of Google v. Costeja

Google v. Costeja sets a milestone in the EU for data protection law with respect to search engines and, more generally, in the online world[99]. It grants data subjects the possibility to request search engines, under certain conditions, the de-listing of links appearing in the search results based on a person's name[100]. To briefly elaborate on the CJEU's answers in its preliminary ruling, we will now quote the Article 29 Data Protection Working Party's[101]

[97] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 93.
[98] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 85.
[99] (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2014) Article 29 Data Protection Working Party - PRESS RELEASE - Adoption of guidelines on the implementation of the CJEU's judgement on the "right to be forgotten" http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2014/20141126_wp29_press_release_ecj_de-listing.pdf
[100] *Id. supra.*
[101] The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The Article 29 Working Party is competent to examine any question covering the application of the data protection directives in order to

executive summary on the "Guidelines on the implementation of the CJEU's judgment"[102] [hereinafter "the guidelines"]. These guidelines contain the common interpretation of the ruling as well as the common criteria to be used by the data protection authorities when addressing complaints[103].

> "1. Search engines as data controllers
> The ruling recognises that search engine operators process personal data and qualify as data controllers within the meaning of Article 2 of Directive 95/46/EC. The processing of personal data carried out in the context of the activity of the search engine must be distinguished from, and is additional to that carried out by publishers of third-party websites.
>
> 2. A fair balance between fundamental rights and interests
> In the terms of the Court of Justice of the European Union (hereinafter: Court, CJEU), "in the light of the potential seriousness of the impact of this processing on the fundamental rights to privacy and data protection, the rights of the data subject prevail, as a general rule, over the economic interest of the search engine and that of internet users to have access to the personal information through the search engine". However, a balance of the relevant rights and interests has to be made and the outcome may depend on the nature and sensitivity of the processed data and on the interest of the public in having access to that particular information. The interest of the public will be significantly greater if the data subject plays a role in public life.
>
> 3. Limited impact of de-listing on the access to information
> In practice, the impact of the de-listing on individuals' rights to freedom of expression and access to information will prove to be very limited. When assessing the relevant circumstances, European Data Protection Authorities (DPAs) will systematically take into account the interest of the public in having access to the information. If the interest of the public overrides the rights of the data subject, de-listing will not be appropriate.
>
> 4. No information is deleted from the original source
> The judgment states that the right only affects the results obtained from searches made on the basis of a person's name and does not require deletion of the link from the indexes of the search engine altogether. That is, the original information

contribute to the uniform application of the directives. It carries out this task by issuing recommendations, opinions and working documents.

[102] (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2014)

[103] (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2014) Article 29 Data Protection Working Party - PRESS RELEASE - Adoption of guidelines on the implementation of the CJEU's judgement on the "right to be forgotten" http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2014/20141126_wp29_press_release_ecj_de-listing.pdf

will still be accessible using other search terms, or by direct access to the publisher's original source.

5. No obligation on data subjects to contact the original website

Individuals are not obliged to contact the original website in order to exercise their rights towards the search engines. Data protection law applies to the activity of a search engine acting as a controller. Therefore, data subjects shall be able to exercise their rights in accordance with the provisions of Directive 95/46/EC and, more specifically, of the national laws that implement it.

6. Data subjects' entitlement to request de-listing

Under EU law, everyone has a right to data protection. In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State.

7. Territorial effect of a de-listing decision

In order to give full effect to the data subject's rights as defined in the Court's ruling, de- listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.

8. Information to the public on the de-listing of specific links

The practice of informing the users of search engines that the list of results to their queries is not complete as a consequence of the application of European data protection is based on no legal requirement under data protection rules. Such a practice would only be acceptable if the information is presented in such a way that users cannot, in any case, conclude that one particular individual has asked for de-listing of results concerning him or her.

9. Communication to website editors on the de-listing of specific links

Search engines should not as a general practice inform the webmasters of the pages affected by de-listing of the fact that some web pages cannot be acceded from the search engine in response to a specific name-based query. There is no legal basis for such routine communication under EU data protection law.

In some cases, search engines may want to contact the original editor in relation to particular request prior to any de-listing decision, in order to obtain additional information for the assessment of the circumstances surrounding that request.

Taking into account the important role that search engines play in the dissemination and accessibility of information posted on the Internet and the legitimate expectations that webmasters may have with regard to the indexing and

presentation of information in response to users' queries, the Article 29 Working Party strongly encourages the search engines to provide the de-listing criteria they use, and to make more detailed statistics available."

Something very important to highlight from the ruling, which the guidelines very adequately echo, is that the RTBF does not entail the right to have content be deleted or erased. Rather, it is a "right to be delisted" (RTBD) from the results of a search performed through a search engine, based on an individual's name. Hence, the "right to be forgotten" label doesn't really fit the court's decision in Google v. Costeja[104]. From now onwards in this dissertation, we will refer to the right conferred in the preliminary ruling as a RTBD.

## 2.3. Critiques and comments on the CJEU's preliminary ruling

As could be expected, the ground-breaking nature of the preliminary ruling in terms of its territorial application, its material scope and the CJEU's recognition of a RTBD within Directive 95/46 resulted controversial to many. Many of the attacks on the decision have been explicitly legal: many critics argue that the court incorrectly found Google a data controller subject to the Directive and that the court's balancing test ignored basic legal principles and rights[105]. Other critics have focused more on the opinion's consequences, arguing that the decision transferred too much power to private entities to "censor the Internet"[106]. Article 29 Data Protection Working Party's guidelines answered many of the critiques that the decision initially received. For this reason, we have only focused in outlining those which still remain relevant after the working party's guidelines and Google's implementation of the decision. In this section, we have synthesised the critiques according to each of the answers in the CJEU's decision.

### 2.3.1. On the territoriality of EU laws

Some critics perceived Google v. Costeja as an unprincipled, unilateral extension of European law. In 2014, the Harvard Law review commented that "left unchecked, the decision bears the risk of submitting all search engine operators – regardless of the location of their headquarters and of the place of their business activities – to the Right to be Forgotten, thus elevating European concepts of personal privacy as the de facto law of the land of the Internet"[107]. This has indeed been the case with other important search engines operating in Europe, such as

[104] (SELINGER, E. & HARTZOG, W., 2015)
[105] (HARVARD LAW REVIEW, 2014, p. 739)
[106] *Id. supra.*
[107] From (REYMOND, 2016), quoting USA Today Editorial Board, America's right to forget the EU: Our view, USA Today, Jan. 22, 2015, http://www.usatoday.com/story/opinion/2015/01/22/right-to-be-forgotten-european-union-google-search-privacy-editorialsdebates/ 22186653/ ("Do Europeans seriously think they're entitled to unilaterally set rules for the entire world?"); Ustaran, supra, at 8-9. Fearing the creation of an European Internet which would have less content than its global counterpart, see Christopher Kuner, The Court of Justice of EU's Judgment on the "Right to be Forgotten": an International Perspective, EJIL: Talk! (May 20, 2014), http://www.ejiltalk.org/the-court-of-justice-of-eus-judgment-on-the-right-to-be-forgotten-an-international-perspective/.

Bing[108]. However, even if the decision has extended to all domains of a search engine, it only extends its effects to searches performed within the EU[109]. Yet, this still raises concerns about lack of homogeneity of individuals' protection outside of the EU. Furthermore, this also revives the debate on the fundamentally different conceptions of privacy between the EU and important countries in the data economy, such as the US[110] or Japan[111].

However, other authors hold that "reaching the opposite conclusion [than the one the CJEU's] would have created an unwanted gap in the scope of the Directive, allowing search engines that knowingly bring their business to the European Union to escape their obligations regarding the search results they publish about European citizens"[112]. Former EU Commissioner for Justice Viviane Reding expressed the same views in stating that:

> "EU law which is agreed by all member states has to be applied by all companies. Not just EU companies, but also those who use our internal market as a goldmine" [113].

Despite effectively protecting EU citizens' RTBD, a full and comprehensive practical implementation of such views would, in fact, entail a universal application of EU data protection laws which would preserve EU citizens' right wherever they went. In its appeal, Google Spain stood not for the universal application of European data protection law, but for the more reasonable proposition that foreign Internet-based businesses that transact with persons located on EU territory are subject to local regulation[114]. As we have seen, this has finally been the case.

Finally, it is important to mention that, overwhelmingly, EU citizens believe that the protection of personal data should not be confined by borders. According to a 2015 European Commission Eurobarometer on data protection, nine out of ten Europeans (89%) believe that

---

[108] SEARCHENGINELAND.COM, Amy Gsesenhues (2016): Bing to censor Bing.com in the EU for Right To Be Forgotten searches http://searchengineland.com/bing-censor-bing-com-eu-right-forgotten-searches-255731

[109] (THE GUARDIAN - Samuel Gibbs, 2016) "Google will begin blocking search results across all of its domains when a search takes place within Europe, in an extension of how it implements the "right to be forgotten" ruling. The "right to be forgotten" ruling allows EU residents to request the removal of search results that they feel link to outdated or irrelevant information about themselves on a country-by-country basis. These edited results will now be shown to anyone conducting name-based searches from the same European country as the original request, regardless of which domain of the search engine the browser is using."

[110] From (REYMOND, 2016), quoting Meg Leta Jones, Ctrl+Z: the right to be forgotten, 47-53 (New York University Press, 2016)., at p. 55-80; Rustad & Kulevska, at 379-380 (showing that there is no all-encompassing right to privacy in the US, which directly clashes against the RTBD).

[111] SEARCHENGINELAND.COM, Greg Sterling (2017): Google wins 'right to be forgotten' case in Japanese high court http://searchengineland.com/google-wins-right-forgotten-case-japanese-high-court-268533

[112] (REYMOND, 2016) quoting Peers ("[I]t would be remarkable if Google, having established a subsidiary and domain name in Spain and sought to sell advertising there, would not be regarded as being 'established' in that country."); Svantesson, supra, at 6-7; van Alsenoy & Koekkoek, supra, at 13. Highlighting that the RTBD, as a right existing between national and regional conceptions of free speech and data privacy, is a "matter of boundary disputes, informed by culture and history", see Julia Powles, Swamplands of the Internet: Speech and Privacy, Ion Magazine (Feb. 11, 2015), http://www.ionmag.asia/2015/02/swamplands-internet-speech-privacy/

[113] Vivian Reding. Former EU commissioner: right to be forgotten is no harder to enforce than copyright. Article by Alex Hern. The Guardian (2014). https://www.theguardian.com/technology/2014/jun/04/eu-commissioner-right-to-be-forgotten-enforce-copyright-google

[114] (REYMOND, 2016, pp. 7-8)

they should have the same level of protection over their personal information, regardless of the country in which the authority or private company processing their data is based[115]. Hence, one could argue that public opinion in the EU very strongly supports the CJEU's decision in terms the territorial applicability of the RTBF.

### 2.3.2. On the applicability of EU data protection laws to a search engine

Other critics, such as Professor Luciano Floridi, Professor at the Oxford Internet Institute of the University of Oxford, express their concerns on the *inclusive and general* definition of "data controller" in the Directive. Given the broadness of the definition, "basically anyone doing anything with data is processing the data, and hence can qualify as a data controller"[116]. This also raises the question on the scope of applicability of the CJEU's ruling to other "controllers" within the meaning of the Directive. In this regard, Prof. Luciano Floridi argues that the Directive (adopted in 1995), which predates Google (founded in 1998) and the world of Social Media, does not appear to distinguish different treatments of data that have only come to exist after the Directive came into place. In his opinion, "the CJEU could and should have interpreted the Directive much more stringently, concluding that a link to some legally available information does not process the information in question"[117]. The House of Lords of the United Kingdom shares the same opinion as Professor Luciano Floridi. In reviewing the decision in a report that fundamentally disagrees with the CJEU's decision, it lamented that the Court's definition of a data controller was now so broad that it could include "any company that aggregates publicly available data"[118].

Other opinions on the applicability of EU data protection laws to search engines call for a more balanced attribution of obligations and rights within the Directive. In this regard, Martin Husovec, affiliate scholar at the Center for Internet and Society at Stanford Law School, focuses on how the exceptions established by the Directive for the use of personal data without the permission of the individual concerned, only comprise the processing "solely for journalistic purposes or the purpose of artistic or literary expression"[119]. He also holds that if we expand the notion of "data controllers" and thus data protection laws, we should also expand exceptions. "Otherwise, we might outlaw socially legitimate processing of personal data and artificially break the chain of speech online"[120]. Thankfully, to alleviate his concerns, art. 17.3 of the GDPR now contains a broader range of exceptions[121].

### 2.3.3. On the right to be delisted (RTBD)

[115] (EUROPEAN COMMISSION, 2015, p. 10)
[116] (FLORIDI, 2014)
[117] (FLORIDI, 2014)
[118] (HARVARD LAW REVIEW, 2014) quoting (European Union Committee, HOUSE OF LORDS OF THE UNITED KINGDOM, 2014)
[119] (HUSOVEC, 2014)
[120] (HUSOVEC, 2014)
[121] In Annex 1.3. of this dissertation.

#### 2.3.3.1. On the balancing of rights that establishes a legal basis for the RTBD

Most of the critiques in terms of the balancing of rights, and in particular, the potential hindering of freedom of expression under the decision, come from the idea that "search engines facilitate the finding of data through the World Wide Web and in consequence, they enhance the ability of individuals to receive and impart information"[122].

Amongst others advocates of freedom of expression, the organisation ARTICLE 19 deeply rejects the general prevalence of the rights to private life and protection of data privacy that the CJEU established over the right to freedom of expression[123]. They argue[124] that the CJEU should have used the criteria established by the European Court of Human Rights' (ECHR) to balance the right to respect for private life against the right to freedom of expression on a case-by-case basis. The balancing criteria that the ECHR established in Von Hannover v Germany (No. 2)[125] assessed:

> "1. Whether the information contributes to a debate of general interest;
> 2. The notoriety of the person concerned;
> 3. The prior conduct of the person concerned and their relationship to the press;
> 4. Content, form and consequences of the publication;
> 5. The circumstances in which the material at issue was obtained (e.g. photograph taken with a hidden camera)."

Regarding the order of priorities that the CJEU established in terms of balancing the rights to private life and to the protection of personal data, Prof. Luciano Floridi believes that:

> "with so many possible exceptions, in terms of security, safety, public interest, relevance, timeliness, roles of the people concerned (e.g. journalists) or involved (e.g. minors), social circumstances (e.g. a former married couple), nature of the information in question (wilfully shared, secretly recorded, publicly available etc.) and so forth, seeking to establish some fixed order of priority is the wrong strategy. By establishing some sort of hierarchical order, but then admitting so many cases in which the rule does not apply, or has exceptions, or is customarily not followed, or has evolved into a different rule, or is overridden by another rule, one is better off by saying that it depends on specific instances, contexts and

[122] (IGLEZAKIS, 2016, p. 4) quoting Search engines after Google Spain: internet@liberty or privacy@peril?, p. 12.
[123] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 97.
[124] (ARTICLE 19, 2014, pág. 5)
[125] Von Hannover v. Germany (no. 2) 40660/08 [2012] ECHR 228 http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=002-98&filename=002-98.pdf

practices, and there is no useful, general way of establishing a priori what comes first and what comes later, but only intelligent and wise discernment"[126].

According to Álvarez Rigaudias[127] this critique is not totally true. She argues that after a careful reading of the preliminary ruling, it is clearly established that such balance "may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life" [128].

Furthermore, Daniel Solove[129], one of the most important academics in the field of privacy law, also criticises the vague justification given by the CJEU when establishing that search engines' sole economic interests could not by itself justify the invasion on data subjects' privacy[130]. He asks, "is the search engine's purpose solely "economic interest"?" And then, he remarks that newspaper companies could arguably also be motivated by economic interests when selling newspapers and providing access to their sites, from which they might receive revenue from ads. "How would all these things be weighed?"[131], he asks.

#### 2.3.3.2. On search engines being responsible for deciding on the RTBD

In Advocate General Niilo Jääskinen's recommendations[132], he stated that, in his view, "the internet search engine service provider cannot in law or in fact fulfil the obligations of controller provided in Articles 6, 7 and 8 of the Directive in relation to the personal data on source web pages hosted on third-party servers"[133]. Despite Google finally being able to fulfil its obligations, Martin Husovec elaborates on this idea in a wider context. He argues that with such obligations being placed on search engines, possible entry barriers are being created in the search engine market[134]. He holds that despite our potential preference for privacy over competition in the search engine market, such market is crucial to the online flow of information and any business online. In this regard, I believe he is referring in particular to the undesirability and dangers of having such an important and sensitive market be controlled by only a very powerful few.

He later elaborates on the idea that having a state authority rule on such conflicts between freedom of expression and privacy would have been desirable, given three main reasons. The

[126] (FLORIDI, 2014)
[127] (ÁLVAREZ RIGAUDIAS, 2014)
[128] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 81.
[129] https://www.law.gwu.edu/daniel-justin-solove
[130] (SOLOVE, 2014)
[131] (FLORIDI, 2014)
[132] (CJEU, 2013)
[133] (JÄÄSKINEN, 2013)
[134] (HUSOVEC, 2014)

first one is that, unlike a private company, "publicly accountable state authorities are directly bound by human rights"[135]. Secondly, "this would also create more legal certainty for service providers and originators of objected speech, given that what is time-relevant for a society is determined and centralised by the state, not industry players"[136]. This would help consistency to be achieved when deciding on particularly difficult cases. Finally, "it would outsource some of the decision-making costs, so the barriers of entry would be lowered"[137]. The examination effort of search engines would thus not be replicated many times, but be centralized to one decision-making process, with positive spill-over on less wealthy competitors[138].

Similar concerns are raised by Dr. Michel J. Reymond, at the Berkman Klein Center for Internet and society at the University of Harvard. He argues that the landscape of the RTBD is thus rather fragmented, since, "in order to scrub results in an efficient matter, a person must simultaneously file the same request with all major search operators, without the guarantee that all of them will agree to the same result"[139].

On the other hand, Edward Lee, professor of Law at the Chicago-Kent College of Law, raises a very valid point about the practicality of delegating the implementation of the RTBF to Google. He points out that no country in the world has the necessary resources to process the huge number of requests[140] on the RTBF. While delegating—or outsourcing—such power to a for-profit corporation raises serious concerns about democratic accountability, there might be no other viable alternative[141].

Lastly, related to this last idea of the concerns about democratic accountability, as The Economist puts it: "the world's most valuable resource is no longer oil, but data"[142]. They argue that "data are to this century what oil was to the last one: a driver of growth and change". [143] While tech giants' success has benefited consumers, there is cause for concern. Internet companies' control of data gives them enormous power[144]. Hence, a radical rethink is required to address such concerns. They argue that is necessary to loosen the grip that providers of online services have over data, and these companies give more control to those

---

[135] *Id. supra.*
[136] *Id. supra.*
[137] *Id. supra.*
[138] *Id. supra.*
[139] (REYMOND, 2016, p. 9): This situation gave rise to services, such as the Forget.me website, allowing claimants to query multiple search engines by filing a single RTBD request. See Frequently Asked Questions, Forget.me, (last visited May 9, 2016), https://forget.me/faq. This quandary has not escaped the European legislator, either, as article 17, par. 2 of the GDPR contains a rule mandating recipients of RTBF requests to "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".
[140] (GOOGLE, 2017) At the moment that sentence was written, Google had received a total of 726,808 requests. https://www.google.com/transparencyreport/removals/europeprivacy/
[141] (EDWARD LEE, 2015)
[142] (THE ECONOMIST - Leaders Section, 2017)
[143] *Id. supra.*
[144] *Id. supra.*

who supply them. Thus, a call for more transparency in the information being held and a further impact of users' consent on the use of their data is required[145]. In the topic that concerns us, giving important search engines the power to decide on the RTBF could further enhance these companies' power in the digital age.

### 2.3.4. The paradox of the CJEU's decision over the RTBD

As some authors[146] have pointed out, there is an interesting paradox in the CJEU's decision over the right to be forgotten. The decision itself contains personal data regarding Mr. Costeja Gonzalez. With the case, more publicity has been given to the information that Mr. Costeja wanted to remove in the first place, regarding the foreclosure auction for the recovery of debts with the Spanish social security in 1998. If we were to make a broad interpretation of the RTBD, "does the plaintiff here have a right to ask the EU Court to remove his name from the decision, as it reveals that he had debts"[147]? If this were the case, how would the opinion be found?[148]

The paradox here is that in winning this landmark case in favour of Internet privacy, Costeja now suffers from the Streisand effect[149] and it is unlikely he will ever be forgotten because his name now appears on thousands of web sites[150] related to the case.

## 3. ON THE "RIGHTS TO BE FORGOTTEN"

While many authors agree the "right to be forgotten" comes as response to the challenge of preserving privacy in the digital age, the meaning and scope of such a right are not as unanimous. Moreover, as we have seen, the "right to be forgotten" label does not exactly fit the court's decision in Google v. Costeja[151].

In this section, we will particularly consider Professors W. Gregory Voss[152] And Céline Castets-Renard's[153] paper: "Proposal for An International Taxonomy on the Various Forms of the "Right to Be Forgotten". According to them, what we call the "right to be forgotten"

[145] *Id. supra.*
[146] (SOLOVE, 2014) and (SELINGER, E. & HARTZOG, W, 2014)
[147] (SOLOVE, 2014)
[148] *Id. supra.*
[149] A phenomenon whereby an attempt to hide a piece of information has the unintended consequence of publicizing the information more widely. (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016)
[150] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 2)
[151] (SELINGER, E. & HARTZOG, W., 2015)
[152] Professor of Business Law, University of Toulouse, Toulouse Business School (TBS), Associate Member of the Institut de Recherche en Droit Européen International et Comparé [Research Institute in European, International and Comparative Law] (IRDEIC), Co-Chair of the American Bar Association Section of International Law Privacy, E-Commerce, and Data Security Committee.
[153] Junior Member of the Institut Universitaire de France and a full Professor at the Université Toulouse 1 Capitole (UT1), Co-Director of the Master in Digital Law at UT1 and Assistant Director of the IRDEIC.

"encompasses several rights to which different legal norms may apply"[154]. Hence, what rights are we really talking about when we talk about the "rights to be forgotten"?

## 3.1. The spectrum of "rights to be forgotten"

Professors W. Gregory Voss And Céline Castets-Renard's paper proposes five main types of rights to be forgotten. To understand these rights, we must first establish a definition of the more general "right to oblivion". According to Professor de Terwangne, "the right to oblivion, equally called right to be forgotten, is the right for natural persons to have information about them deleted after a certain period of time" [155]. With this definition of oblivion in mind, the rights identified in Voss & Renard's paper are:

> "1. **Right to rehabilitation**: the right to oblivion of the judicial past;
> 2. **Right to deletion/erasure**: the right to oblivion established by data protection legislation;
> 3. **Right to delisting/delinking/de-indexing**; a form of digital right to oblivion with respect to search results referencing a natural person.
> 4. **Right to obscurity**; and
> 5. **Right to digital oblivion of data collected by information society services**: "digital right to oblivion that amounts to personal data having an expiration date or being applicable in the specific context of social networks.""

The important difference between these rights, according to Voss & Renard, is that the first two rights listed above are not linked to the digital age, in contrast to the last three, which appear later in a digital context[156]. The last two rights come as a result of information society services[157]. In their paper, the authors place the first group in what they call the "general context" of the right to be forgotten, prior to the later "digital context".

Before we elaborate on each of these "rights to be forgotten" it is important to note that their application always requires balancing tests with other rights or interests. The different scaling of the "rights to be forgotten" is very relevant in this regard. A less "intense" or "protective" RTBF, for example, might be more conciliatory with a legitimate public interest, as opposed to one which could allow for the deletion or "auto-expiry" of data. As Peter Fleischer, Global Privacy Counsel for Google also points out, "sometimes people aren't trying to delete content, they're just trying to make it harder to find"[158]. This is particularly significant, since it could

[154] (W. G. VOSS & C. C. RENARD, 2016, p. 8)
[155] (W. G. VOSS & C. C. RENARD, 2016) quoting Cécile de Terwangne, Internet Privacy and the Right to Be Forgotten/Right to Oblivion, 13 REVISTA DE INTERNET, DERECHO Y POLÍTICA 109, 110 (2012).
[156] (W. G. VOSS & C. C. RENARD, 2016) quoting Cécile de Terwangne, Internet Privacy and the Right to Be Forgotten/Right to Oblivion, 13 REVISTA DE INTERNET, DERECHO Y POLÍTICA 109, 110 (2012).
[157] (W. G. VOSS & C. C. RENARD, 2016): "Information society service" is the term used in Europe, under EU law, to refer to "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services." Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 Amending Directive 98/34/EC Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations, 1998 O.J. (L. 217) 18, 21 art. 1(2)(a)(2)
[158] (PETER FLEISCHER, 2011)

provide some common grounds for a global regulation on the RTBF, which could somewhat conciliate fundamentally different conceptions of privacy.

### 3.1.1. Right to rehabilitation

The right to rehabilitation guarantees a right to social reintegration after a judicial conviction[159]. It is the right to oblivion of the judicial past[160]. It recognizes that, under certain circumstances, it may be appropriate to grant a pardon to a person who has been convicted of a criminal offense, "after a certain period of time following such conviction and after such person, who has evidenced good behavior, has served his or her sentence"[161]. This right is present in Europe, as well as outside of Europe[162].

### 3.1.2. Right to deletion/erasure (or to delete)

According to the authors, the right to deletion became more widespread after the establishment of the Organization for Economic Cooperation and Development (OECD) Privacy Principles contained in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)[163]. Paragraph 13 of the OECD Guidelines encompasses individuals' right "to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended"[164].

Within the EU, the right to erasure is defined in art. 6(1)(d) of Directive 95/46:

> "Member States shall provide that personal data must be: (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified."

Hence, we could define the "right to erasure" as the right to have personal data erased when it is not accurate or necessary for the purposes for which they were collected. In former EU Commissioner Viviane Reding's words: "if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system"[165]. In this regard, "right of erasure" is now enshrined in art. 17 of the GDPR as the "right to be forgotten"[166].

### 3.1.3. Right to delisting/delinking/de-indexing

---

[159] (W. G. VOSS & C. C. RENARD, 2016, p. 299)
[160] *Id. supra.*
[161] *Id. supra.*
[162] *Id. supra.*
[163] (W. G. VOSS & C. C. RENARD, 2016, p. 302)
[164] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm . The OECD Guidelines were updated in 2013, but we will refer to the original 1980 version.
[165] (REDING, 2012)
[166] In Annex 1.3. of this dissertation.

The right to delisting is sometimes also referred to as the "right to delinking" or the "right to de-indexing". When talking about the right to be forgotten in the context of Google v. Gosteja, this is the right recognised by the CJEU through the interpretation of arts. 2(b) and (d), 4(1)(a) and (c), 12(b) and (a), 14(a) of the Data Protection Directive[167], and arts. 7 and 8 of the EU Charter of Fundamental Rights[168].

In contrast with the more extensive "right to erasure", the "right to delisting" entails the right of individuals to request from search engines the removal of links to personal information about them. This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing[169]. This right operates in the context of search engines' processing of personal data and, which are considered as "controllers" under Directive 95/46[170]. Furthermore, the right to delisting can be enforced without individuals also having to address the publishers of the information concerning them on third-party websites, to which links are provided in the search engine results[171]. The CJEU's decision involves a mere right to delisting (and not to be completely forgotten) because the court orders the erasure of web links, but not the related article. In other words, "the source is preserved"[172]. Finally, in order to recognize a right to delisting, neither the economic interest of the operator of the search engine nor the interest of the general public in having access to that information shall prevail over the data subject's reputation and privacy[173].

### 3.1.4. Right to obscurity

The relevance of the right to obscurity comes in the context of the traditionally different approaches to privacy in the EU and the US[174]. In the context of the First Amendment of the US Constitution[175], enshrining freedom of expression, it would be very difficult to imagine a RTBF with such an extended scope as the one recognised in the EU[176]. However, the right to obscurity could be an acceptable form of the "right to be forgotten" in the United States.

As US Federal Trade Commissioner Brill stated: "obscurity means that personal information isn't made readily available to just anyone. It doesn't mean that information is wiped out or even locked up; rather, it means that some combination of factors makes certain types of information relatively hard to find"[177]. According to Hartzog and Stutzman[178], "information is

[167] In Annex 1.2. of this dissertation.
[168] See ANNEX section 1.1.
[169] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 92.
[170] *Id. supra* paragraph 33.
[171] *Id. supra* paragraph 77.
[172] (W. G. VOSS & C. C. RENARD, 2016, p. 326)
[173] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 81.
[174] (U.S. Federal Trade Commissioner Julie Brill, 2014)
[175] (ROSEN, 2012)
[176] (W. G. VOSS & C. C. RENARD, 2016, p. 335)
[177] (U.S. Federal Trade Commissioner Julie Brill, 2014)

obscure online if it lacks one or more key factors that are essential to discovery or comprehension." According to the authors, such factors are: "(1) search visibility; (2) unprotected access; (3) identification; and (4) clarity"[179]. They have argued that the "right to obscurity" in cyberspace should be easier to implement than the more vague "right to privacy" or to define the "breaches of the right to privacy" in cyberspace[180]. "Obscurity could also serve as a compromise protective remedy: instead of forcing websites to remove sensitive information, courts could mandate some form of obscurity"[181]. This right is very interesting, because it could play a more important role in U.S. federal legislation than the "right to be forgotten" which may conflict with the "freedom of speech" clause of the First Amendment of the U.S. Constitution[182]. Finally, it is important to mention that this right is not yet recognized in law[183].

### 3.1.5. Right to digital oblivion of data collected by information society services

According to Voss & Renard, the "right to digital oblivion of data collected by information society services[184]" comes as a response to the social demand to delete certain personal information collected by information society services. Such a right "would allow an individual to request that social networks, browsers, and servers suppress or cancel his or her personal information contained in their databases"[185]. In the case of contractual relationships with institutions that offer goods and services and collect personal information, individuals could request that their personal information is cancelled once the contractual relationship ends[186].

Voss & Renard argue that the right to oblivion of data collected by information society services is "a real right to be forgotten" which can be exercised without the condition of providing evidence. It is not necessary to prove that the data are irrelevant, out-of-date, or illegal[187]. Besides, it is not merely a right to obscurity, because the data are deleted[188]. Therefore, it is a broad right to obtain the erasure, meeting a social demand for this right, especially with respect to social networks[189].

In this regard, one could argue that such a right would be widely supported by EU citizens. In the European Commission's 2015 Eurobarometer on data protection, respondents had serious questions about the consequences of their data being collected, processed and used. Seven out

[178] (HARTZOG, W. & STUTZMAN, F., 2013, pág. 334)
[179] *Id. supra.*
[180] *Id. supra.*
[181] *Id. supra.*
[182] (W. G. VOSS & C. C. RENARD, 2016, p. 335)
[183] *Id. supra.*
[184] Definition in footnote 157.
[185] *Id. supra.*
[186] *Id. supra.*
[187] (W. G. VOSS & C. C. RENARD, 2016, p. 336)
[188] *Id. supra.*
[189] *Id. supra.*

of ten people are concerned about their information being used for a different purpose from the one it was collected for[190] and nearly seven out of ten people (69%) said that their explicit approval should be required in all cases[191].

### 3.1.6. Comparative table of the "rights to be forgotten" by Voss & Renard[192]

| CRITERIA | **RIGHT TO REHABILITATION (General Context)** | **RIGHT TO DELETION (PERSONAL DATA LEGISLATION) (General Context)** | **RIGHT TO DELISTING (Digital Context)** | **RIGHT TO OBSCURITY (Digital Context)** | **RIGHT TO DIGITAL OBLIVION (Digital Context)** |
|---|---|---|---|---|---|
| **Where and who?** | Examples:<br>French Law: Criminal Code, Art. 133- 12<br>UK Law: Rehabilitation of Offenders Act<br>US Law: Fair Credit Reporting Act (FCRA) | Examples:<br>French Law: Data Protection Act<br>EU: Data Protection Directive<br>Europe: Council of Europe Convention 108<br>US: Specific Federal legislation/Specific State legislation | Examples:<br>EU: Google Spain Case (case law)<br>Russia: delisting law<br>Israel: amendment bill to the Privacy Act (PPA)<br>Brazil: Bill no. 7881/2014 | US: draft Data Broker Accountability and transparency Act of 2015 | Nicaragua<br>EU: GDPR and Council of Europe's recommendation<br>US: California "Erasure Law" in favour of minors<br>US: State legislation on "revenge porn". |
| **Exercised by whom?** | The ex-offender data subject | The data subject | The data subject | The data subject | The data subject |
| **Of general or specific application?** | Specific in a context of judicial past in the aim of social rehabilitation | France, EU, and Asia: general<br>US: specific | Specific | Specific | Specific |
| **Source?** | Criminal Law | Personal data legislation | Case law in Europe<br>Case law in certain other countries | Federal law | Law |
| **Limited to a certain age?** | No | No | No | No | It could be: California Law on right to be forgotten is limited in favour of minors |
| **Conditions on data?** | No | Incomplete, irrelevant, inaccurate, or up-to-date information | Several criteria: not public life, minor, irrelevant, inaccurate, or up-to-date information | Data used in a marketing purpose | Specific context: data collected by information society services (especially social networks)<br>Specific content: revenge porn |
| **Absolute right or balancing against other interests?** | No, but strict legal conditions | No, but legal conditions on data and evidence | No, but balancing with the freedom of speech | Yes, but only a right to obscurity in a commercial use | Yes, but in specific circumstances |

[190] (EUROPEAN COMMISSION, 2015, p. 17)
[191] (EUROPEAN COMMISSION, 2015, p. 27)
[192] (W. G. VOSS & C. C. RENARD, 2016, pp. 338-339)

## 3.2. Implementing the RTBD: how and what are we forgetting?

Thanks to the CJEU's decision in Google v Costeja, Google was obliged to delist certain links related to Mr. Costeja when a search was made on the basis of his name. As we have pointed out, the right observed in this case would fall under the more accurate label of a RTBD. Now that we have seen the different modalities of the RTBF, in this section we will outline Google's process for the removal of links. Furthermore, we will also look at a data study which shines a light on the types of data that are being delisted from Google's searches.

### 3.2.1. How Google processes individuals' requests over the RTBD

To request the removal of links from European Google sites, individuals must first complete a web form provided by Google[193]. Since Google began accepting requests on May 29, 2014, Google has received 727,630 requests for the removal of 2,055,546 URLs, as of May 27, 2017[194]. Once the requests are received, a committee at Google assesses each request on a case-by-case basis to determine whether the URLs should be removed[195].

Google's evaluation process follows criteria aligned with the Article 29 Working Party's guidelines for the implementation of Google v Costeja and it consists of four steps[196]:

> "1. Does the request contain all the necessary information for us to be able to make a decision?
> 2. Does the person making the request have a connection to a European country, such as residency or citizenship?
> 3. Do the pages appear in search results for the requester's name and does the requester's name appear on the page(s) requested for delisting?
> 4. Does the page requested for removal include information that is inadequate, irrelevant, no longer relevant, or excessive, based on the information that the requester provides? Is there a public interest in that information remaining available in search results generated by a search for the requester's name?"

URLs are typically removed for the following types of requests[197]:

> "- Private or sensitive information, such as pages that contain information about personal contact, address, health, sexual orientation, race, ethnicity, and religion.
> - Content that relates to minors or to minor crimes that occurred when the requester was a minor.

[193] Google FAQ. Google frequently asked questions: European privacy in search. https://www.google.com/transparencyreport/removals/europeprivacy/
[194] (GOOGLE, 2017)
[195] *Id. supra.*
[196] *Id. supra.*
[197] *Id. supra.*

- Acquittals, exonerations, and spent convictions for crimes. Google tends to delist content relating to a conviction that is spent or accusations that are proven false in a court of law."

On the other hand, Google may decline to delist if it determines that the page contains information which is of public interest[198]. To assess whether such public interest is present, Google analyses diverse factors such as: whether the content relates to the requester's professional life, a past crime, political office, position in public life, or whether the content itself is self-authored content, government documents, or journalistic in nature[199]. If an individual's request for removal is denied he or she may request that a local data protection authority reviews Google's decision[200].

URLs are only delisted in response to queries relating to an individual's name. So, if Google grants a request to delist an article for John Smith about his trip to Paris, Google would not show the URL for queries relating to [john smith] but would show it for a query like [trip to paris].

A key point about Google's removal process is that it notifies webmasters when pages from the webmasters' sites are delisted. However, it only sends the affected URLs and not the requester's name[201].

### 3.2.2. What are we forgetting: "The Right to be Forgotten in the Media: A Data-Driven Study"?

To give a more empirical-based assessment of Google's implementation of the RTBF, we will reference Minhui Xue, Gabriel Magno, Evandro Cunha, Virgilio Almeida, and Keith W. Ross' work "The Right to be Forgotten in the Media: A Data-Driven Study".

As we have pointed out before, Google informs webmasters when links to their sites are delisted. A number of media sites in the UK (oddly uniquely in the UK), upon receiving these notifications, republish the URLs, "in the name of transparency and full disclosure"[202]. As of December 2015, the BBC, the Telegraph, the Daily Mail, and the Guardian have republished a total of 283 delisted links to articles, which constitute the authors' basic sample for the study. For each of the 283 delisted links, the authors downloaded, analysed and manually classified the articles into 18 different categories.

Their main findings in analysing the delisted articles were:

[198] *Id. supra.*
[199] *Id. supra.*
[200] *Id. supra.*
[201] *Id. supra.*
[202] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 3)

- The majority of the 1.5 million URL removal requests to date[203] are for pages on social media and profiling sites that contain private personal information such as email address, home address, health, sexual orientation, race, ethnicity, religion, and political affiliation[204].
- In particular, each of the eight sites for which Google receives the most requests are either social media or profiling sites, and 95% of the requests are for delisting of URLs pointing to private information[205].
- In general, they see that many of the delisted topics treat highly sensitive topics, including sexuality, sexual assault, murder, paedophilia, financial misconduct, terrorism, and so on[206].
- There are four topics related to sexuality, which are "Sexual Assault," "Prostitution," "Paedophilia" (typically involving interactions between adults and minors), and "Sexual Miscellaneous." (If the article discusses a sexual incident but has nothing to do with assault, prostitution, or paedophilia, they categorise it into "Sexual Miscellaneous.") Articles in "General Miscellaneous" are largely mundane topics related to sports, education, and so on. "Non- textual" consists of non-textual documents such as images[207].

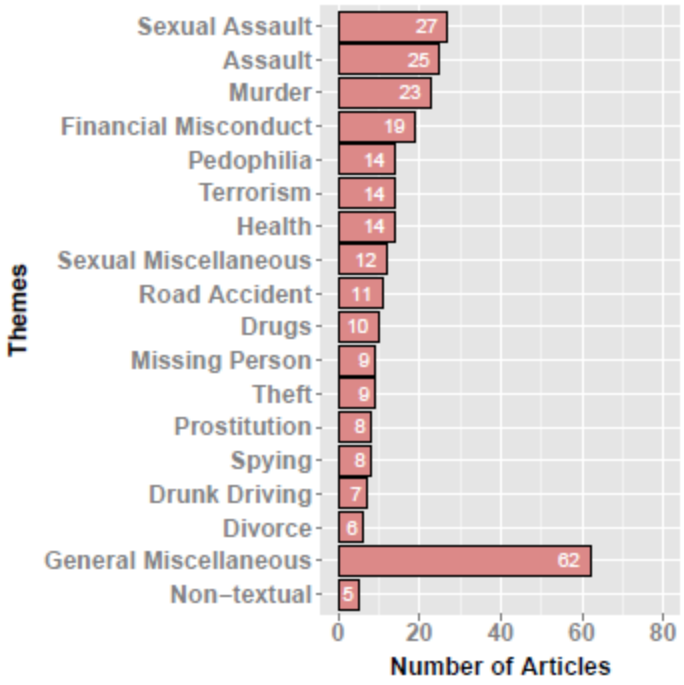
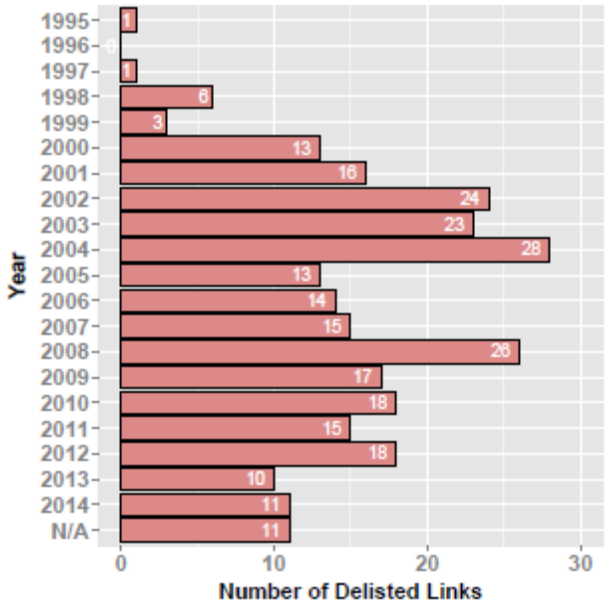



**Fig. 3.** Distribution of articles by theme

[203] To the date in which the study was carried out.
[204] *Id. supra.*
[205] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016) quoting S. Tippmann and S. Pamiés. Google's data on the right to be forgotten. http://sytpp.github.io/rtbf/index.html, 2015.
[206] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 6)
[207] *Id. supra.*

- Most likely Google accepted to delist many of these sensitive articles due to spent convictions, accusations that are proven false in a court of law, or content relating to a criminal charge for which the requester was acquitted[208].
- Strikingly, 87.5% (70 out of 80) of the requesters are male, which seems to imply that males are more inclined to make RTBF requests than females. However, this result is potentially biased by the fact that males may be mentioned more often than females in the mass media[209].
- The dates of publication of the relisted articles range from 1995 to 2014, with the large majority appearing between 2000 and 2012[210].



(b) Distribution of delisted links by year

In their conclusions, the authors "feel that RTBF has been largely working and responding to legitimate privacy concerns of many Europeans"[211]. They also considered that "Google's process for determining which links should be delisted seems fair and reasonable"[212]. Furthermore, they believe that Google is being "fairly transparent about how it processes RTBF requests", as by being more specific about how the delisting decisions are made, it may become easier to rediscover delisted URLs and the corresponding requesters[213]. However, they do point out that other academics have called for more transparency[214].

[208] *Id. supra.*
[209] *Id. supra.*
[210] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 4)
[211] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 13)
[212] *Id. supra.*
[213] *Id. supra.*
[214] E. P. Goodman. Open letter to Google from 80 Internet scholars: Release RTBF compliance data. https://medium. com/@ellgood/open-letter-to-google-from-80-internet- scholars-release-rtbf-compliance-data-cbfc6d59f1bd#

In their study, they also issued some recommendations to improve Google's delisting process. In this regard, they recommend that Google desists from notifying the webmasters about their delisted content[215]. As they observed, this may result in the republishing of the links by media companies acting as transparency activists[216]. Furthermore, they also identified that many of the requesters can be identified from the republished delisted links, thereby possibly generating a Streisand effect[217].

Despite their study providing us with some valuable insight into the practical implementation of the RTBD and "what we are forgetting", we must proceed with caution in drawing our own conclusions from the study. As we have seen, the sample is very limited in comparison to the total requests received. Furthermore, it only provides us insight into the news published by UK media companies, which could arguably mostly affect only individuals living in or somehow related to the UK. However, it is very important to point out that most of the requests analysed in the study were related to some kind of past criminal offense or felony. This raises the question of whether the right to be delisted could actually really be more related to the principle of criminal rehabilitation than initially thought. In this regard, could future reforms of criminal legislations also have an impact on the right to internet privacy? Should these kinds of reforms also take into consideration a possible "expiry date" or "obscurity" for such information, as is the case now with some criminal registries?

## 3.3. Further developments on the "rights to be forgotten": adaptation, present and future of the RTBF

In this last section, we will look into three major developments regarding the RTBF since Google v. Costeja: the extension of the decision to all of Google's domains, the Manni case and art. 17 of the GDPR.

#### 3.3.1.1. Adapting the "universal virtual reach" of the RTBD

Right after Google started implementing the RTBD, it only applied it to searches within its European versions of Google (for example, within google.fr or google.uk), but not to the US site google.com[218]. Thus, when a search within Europe was made on google.com with the requester's name, the links to the RTBD-delisted content would continue to appear[219]. This practice hindered the effectiveness of the CJEU's decision, given that google.com was still accessible to any European[220]. As a response to this, the French data protection authority

[215] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 13)
[216] *Id. supra.*
[217] *Id. supra.*
[218] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 1)
[219] *Id. supra.*
[220] (XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W., 2016, p. 2)

ordered Google to delist links from all its domains, including google.com[221]. In this regard, the Article 29 Data Protection Working Party's guidelines also clearly stated that the decision should have effects on all Google's domains[222].

Despite initially refusing, Google finally extended the RTBD to all of its domains[223]. However, it is important to highlight that Google v. Costeja still only extends its effects on searches performed within the EU[224].

### 3.3.2. Present: The Manni Case and the RTBF in regard to company registries

In July 2015, the Italian Supreme Court asked the CJEU for a preliminary ruling regarding a possible "right to obscurity" in the context of company registries. Instead of focusing on the third-party like in Google v Costeja, this time the CJEU was asked to evaluate the obligations of the original publisher. The issue at stake here was whether the source could be asked to make certain information less accessible[225]. The case raised very interesting questions which were not answered in Google v. Costeja, such as the extent of the original publishers' obligations towards data subjects and the different degrees of publicity of the original publishing[226]. The CJEU ruled on the case on the 9th of March 2017.

#### 3.3.2.1. The facts

Mr Salvatore had been the sole director of a company that went bankrupt in 1992. This information was kept in the companies register of the Lecce Chamber of Commerce, under the guidelines established by Directive 68/151[227]. This Directive aimed at ensuring disclosure of the identity and respective functions of persons with administrative powers in companies.

According to Mr. Salvatore, the inclusion of his personal data in the companies register for the bankruptcy of his previous company caused damage to his reputation. Because of this

---

[221] CNIL. CNIL orders Google to apply delisting on all domain names of the search engine. http://www.cnil.fr/english/newsand-events/news/article/cnil-orders-google-to-applydelisting-on-all-domain-names-of-the-search-engine/, 2015.

[222] (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2014, pág. 3)

[223] (THE GUARDIAN - Samuel Gibbs, 2016) "Google will begin blocking search results across all of its domains when a search takes place within Europe, in an extension of how it implements the "right to be forgotten" ruling. The "right to be forgotten" ruling allows EU residents to request the removal of search results that they feel link to outdated or irrelevant information about themselves on a country-by-country basis. These edited results will now be shown to anyone conducting name-based searches from the same European country as the original request, regardless of which domain of the search engine the browser is using."

[224] *Id. supra.*

[225] (AUSLOOS, 2015)

[226] (AUSLOOS, 2015)

[227] First Council Directive 68/151/EEC of 9 March 1968 on co-ordination of safeguards which, for the protection of the interests of members and others, are required by Member States of companies within the meaning of the second paragraph of Article 58 of the Treaty, with a view to making such safeguards equivalent throughout the Community. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31968L0151

damage, his new company was not able to sell some properties in a tourist complex, which he had been awarded the development of. He then filed a request to erase, anonymise or block the data linking him to the liquidation of his previous company from the registry, but the Lecce Chamber of Commerce denied it.

The case reached the Corte Suprema di Cassazione (Italian Supreme Court), which decided to ask the CJEU for a preliminary ruling. The Italian Supreme Court essentially asks whether such information can be erased, anonymised or access-restricted after a certain time. Another key aspect in this case was also the question of whether Article 6(1)(e)[228] of the Directive 95/46 displaced the requirement of publicity for persons with administrative powers in companies, set by Directive 68/151 and the provisions of national laws which transposed Directive 68/151.

#### 3.3.2.2. Main points and decision

- The processing of personal data by the authority responsible for keeping the register was legitimated under the compliance with a legal obligation, under Directive 68/151[229].
- Even after the dissolution of a company, rights and legal relations relating to it continue to exist. Thus, in the event of a dispute, the data referred to in Article 2(1)(d) and (j) of Directive 68/151[230] may be necessary to assess the legality of acts carried out on behalf of the liquidated company or to bring actions against the administrators or liquidators of that company[231].
- Given the considerable heterogeneity in the limitation periods established in national laws, "it seems impossible" to establish a single time limit after which the inclusion of such data in the register and their disclosure would no longer be necessary[232].
- The natural persons referred to in Article 2(1)(d) and (j) of Directive 68/151 do not have a general right to obtain the erasure of personal data concerning them, or to request the blocking of that data from the public, after a certain period of time from the dissolution of the company concerned[233]. Such interpretation does not result in disproportionate interference with the right to respect for private life and the right to protection of personal data of the persons concerned given that:
    - Disclosure is only required for a limited number of personal data items: the identity and the respective functions of persons having the administrative powers to bind the company or of those having been appointed as liquidator of that company)[234].

[228] In Annex 1.2. of this dissertation.
[229] (Camera di Commercio di Lecce v Salvatore Manni, 2017) paragraph 42.
[230] In Annex 1.4. of this dissertation.
[231] *Id. supra* paragraph 53.
[232] *Id. supra* paragraph 55.
[233] *Id. supra* paragraph 56.
[234] *Id. supra* paragraph 58.

    - Directive 68/151 provides for disclosure of the data given that the only safeguards that companies offer to third parties are their assets, which constitutes an increased economic risk for the latter[235].
- The need to protect the interests of third parties in relation to companies and to ensure legal certainty, fair trading and the proper functioning of the internal market override the provisions of art. 14(a) of Directive 95/46. However, there may be specific situations which can justify a limitation of the access to personal data entered in the register[236].
- The final decision regarding the applicability of art. 14(a) of Directive 95/46 and, hence, the limitation of access to personal data, concerns the authority responsible for keeping the register. Such decision must be taken on the basis of a case-by-case assessment. Specific regulation over such limitation is a matter for the national legislations[237].

#### 3.3.2.3. Comment on the decision

This case is relevant in that it provides a more accurate scope for the RTBF by establishing a more concrete balancing of rights. However, it is interesting to observe how, in this case, the CJEU gave a greater value to the protection of third parties' economic interests within the internal market over individuals' right to privacy.

If we compare the nature of the information in Costeja and Manni, we could argue that they both share the same the same potential negative consequence for the individuals concerned, given that the publicity of certain information could affect their capacity to engage in future economic activity. However, in our opinion, the main difference lies in the level of publicity of the information for each of the cases. In Costeja, the information was virtually accessible to anyone who typed in Mr. Costeja's name on a search engine, while in Manni the specialised nature of the companies' registry already limits the visibility of such information.

Furthermore, it is also interesting to see how the CJEU once again externalised the decision power over a "right to erasure" or a "right to obscurity". In any case, we do however share the CJEU's argument that it would indeed prove almost "impossible" to establish a single time limit after which the inclusion of such data in the register and their disclosure would no longer be necessary.

Lastly, the case already reflects the importance of the GDPR regarding the different modalities of the RTBD. According to Denis Kelleher[238], the Manni case seems consistent with the new Article 17 of the GDPR, given that:

[235] *Id. supra* paragraph 59.
[236] *Id. supra* paragraph 60.
[237] *Id. supra* paragraph 61.
[238] (KELLEHER, 2017)

"It provides that subjects may seek the erasure of their personal data where that data is "no longer necessary in relation to the purposes for which they were collected[239]". However, subjects will not be able to obtain the erasure of their personal data where processing is necessary "for compliance with a legal obligation[240]". Hence, if the retention of data is required by law then the RTBF cannot be invoked, unless that law limits the time for which data may be retained."

### 3.3.3. The future of the RTBF: Article 17 of the GDPR

The General Data Protection Regulation, which will come into force from May 2018, will arguably provide further grounds for the debate on the RTBF. The regulation was first proposed in 2012 and was finally approved in April 2016. The regulation comes as a response to the "challenges brought by rapid technological developments and globalisation"[241]. Furthermore, it aims to ensure a "strong and more coherent data protection framework in the Union"[242]. In other words, it answers the need for an updated, comprehensive and harmonizing regulation on data protection within the EU.

In this regard, the "right to be forgotten" is now explicitly regulated in the provisions of art. 17 of the GDPR. This article basically includes a "right to erasure" of data that requires the controller to delete personal data and preclude any further dissemination of this data, but also to oblige third parties, e.g. search engines, etc., to delete any links to, or copies or replication of that data[243]. This applies in six instances, which derive from data protection principles[244]:

"(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, and where there is no other legal ground for the processing;
(c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing;
(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 to children."

---

[239] Art. 17(1)(a) in Annex 1.3. of this dissertation.
[240] Art. 17(3)(b) in Annex 1.3. of this dissertation.
[241] Recital 6 of the preamble of the GDPR: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en
[242] Recital 7 of the preamble of the GDPR: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en
[243] (IGLEZAKIS, 2016, p. 3)
[244] Costa, L./Poullet, Y., Privacy and the regulation of 2012, (2012) Computer Law & Security Review 28, pp. 254-262.

Furthermore, controllers who have made data public, which is then subject to a right to erasure request, are now required to notify others who are processing that data with details of the request[245]. This is a new wide-ranging and challenging obligation[246], which could also raise questions about the responsibilities of third parties in implementing the RTBF.

The "RTBF" which is enshrined in the GDPR is also restricted by several, more concrete, exceptions than those previously found in art. 9 of Directive 95/46[247]:

> "Member States shall provide for exemptions (…) for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."

Under art. 17(3), these exceptions now are[248]:

> "- for exercising the right of freedom of expression and information;
> - for compliance with a legal obligation set by EU or Member State law;
> - for the performance of a task carried out in the public interest or in the exercise of official authority;
> - for reasons of public interest regarding public health;
> - for archival, scientific, historical, research or statistical purposes
> - for the establishment, exercise or defence of legal claims."

The GDPR has the merit of emphasising this "right to be forgotten" and making explicit what one might have previously deduced from the guiding data protection principles[249] and the CJEU's doctrine. However, Voss & Renard consider that the GDPR has not fundamentally changed the situation existing under the Data Protection Directive[250]. Furthermore, they point out that there is no new "right to be forgotten" under the GDPR, but "merely a right to have the data destroyed when they are out of date, obsolete, irrelevant, or excessive considering the purpose of the processing"[251].

[245] (BIRD & BIRD, 2017, pág. 28)
[246] *Id. supra.*
[247] In Annex 1.2. of this dissertation.
[248] (BIRD & BIRD, 2017, pág. 29)
[249] (W. G. VOSS & C. C. RENARD, 2016, p. 307)
[250] *Id. supra.*
[251] *Id. supra.*

# CONCLUSIONS

The aim of this final dissertation was to present a general overview of the right to be forgotten. Given the structure followed in this dissertation, our conclusions will first assess subjects that we discussed under the Google v. Costeja section, followed those discussed under the section on the "right to be forgotten"

In all, we agree with the need for the existence of a RTBF. However, we hold concerns about some aspects of its current implementation. Moreover, we also recognise the need for more insight into the types of subjects that should be prone to being forgotten.

## 1. On the territorial and material scope of application of EU data protection laws

Despite finding many of the critiques to the decision very valid and insightful, we fundamentally agree with the CJEU's interpretation that a right to be forgotten was indeed rooted in Directive 95/46. With privacy being recognised as a fundamental right in the EU, we believe it was necessary for the Directive to be interpreted in line with guaranteeing the effective protection of such right. As such, we agree with the CJEU's decision that the Directive was territorially and materially applicable to Google. However, we have more doubts regarding the balancing of rights established in the RTBD and how the CJEU prescribed its implementation.

## 2. On the balancing of rights under the "rights to be forgotten"

On the balancing of rights, one of the first lessons we received as Law students was that fundamental rights have no hierarchical order between them. It is in the assessment of the conflict between fundamental rights that we can establish whether one has a justified prevalence over another. We recognise that given our sole basic knowledge on the issue, authors might currently be taking a different stance from the one we were taught. However, from a technical perspective, it surprised us that the CJEU established a general prevalence of the rights to private life and protection of data privacy over the general public's interest in accessing certain information. We do understand that in doing so, the CJEU wanted to ensure the maximum effectiveness of individuals' right to privacy, however, we think that procedurally it was probably not the best technique.

Further, this was surprising in the Manni case, where the CJEU seemed to take a step back in recognising that limiting individuals' right to privacy was justified in safeguarding the economic interests of the internal market. As previously said, we identified that the dangers or harms of having certain data be public in Costeja and Manni were very similar. In our opinion, rather than establishing a dangerous precedent in the balancing of economic interests v. privacy, the CJEU should have focused on the publicity of the data being contested in both cases and the specific people which might have an interest in having access to such information. By taking this approach they would have concluded that such information being held in a specific registry, which is normally only consulted by individuals or institutions

engaging in economic activity, already provides more "obscurity" to such information. This approach could have led to same result, further clarifying the CJEU's doctrine on the RTBF by recognising the spectrum of "rights to be forgotten" while also establishing the scope of a "right to obscurity".

## 3. On the implementation of the "rights to be forgotten" by search engines

We believe that search engines should still be able to directly implement the RTBD, however, they should be held more accountable in their implementation. As we pointed out earlier, data has become one of the most important economic resources of our time. Given that information is so intrinsically linked to the fundamental right to privacy, we believe that further regulatory action must be taken. In this regard, it is quite surprising that the same private institution that earns economic benefit from the processing of our data is responsible for deciding on erasing or delisting our information. However, as we have observed in Google's reports on the RTBD requests, the great number of requests would indeed make it very difficult for any state jurisdiction to handle that workload. Hence, in the implementation of the RTBF/RTBD insofar as they concern big-scale private entities, we see the need for a hybrid system of review.

In our ideal scenario, Google or other search engines would serve as a first instance that is legally bound by guidelines decided on by public entities. They would also be required to systematically report on the types of requests that they accept and those that they deny. In case of non-compliance with such guidelines, sanctions could be imposed on the companies. If individuals are not satisfied with the private entities' resolution then state data protection agencies or institutions could serve as a second instance. The system that we have outlined is very similar to the one in place now. However, the most important difference lies in the transparency of private companies' implementation and the binding force of state institutions' guidelines.

## 4. On the developments and future of the "rights to be forgotten"

One of the main critiques to Google v. Costeja was the broad interpretation and general wording used by the CJEU. While this initially generated some legal uncertainty over the decision, we believe that CJEU was correct in doing so. As we have seen, the need for a new, updated regulation on data protection led to the proposal of a new GDPR in 2012. Thus, Google v. Costeja is found in a transitory context between the Directive and the new GDPR. We believe that in making its decision so broad, the CJEU gave room for the European legislators to embody a more concrete RTBF in the Regulation. We saw that that was finally the case, as art. 17 of the Regulation is now more conceptually comprehensive. In this regard, we applaud the inclusion of the different exceptions to the application of the RTBF. It remains to be seen, however, how the new art. 17 will be put into practice given the previous balancing criteria established by the CJEU.

But even though art. 17 of the GDPR has now explicitly embodied the RTBF, much more remains to be done. As we have seen, the more general term of "RTBF" actually encompasses several rights. The different aims pursued by each of these "rights to be forgotten" could be very relevant in providing different and more precise solutions in balancing privacy v. public interest in different situations. A less "intense" or "protective" RTBF, for example, might not be as invasive over a legitimate public interest as one which allows for the deletion or "auto-expiry" of data. In the Manni case, the CJEU had the opportunity to recognise the spectrum of rights to be forgotten as a possible general and more precise solution. However, it failed to do so.

By recognising the spectrum of RTBF we could also make another global ground-breaking advance. As we have seen, traditionally there have been different conceptions of privacy between the EU and important countries in the data economy, such as the US or Japan. Given the global impact of the internet, data protection nowadays requires collaborative efforts in guaranteeing individuals' right to privacy. If we were to recognise the different rights to be forgotten, it is less unreasonable to think that some kind of international conciliatory framework on data privacy could be reached.

## 5. On the value of forgetting with the "rights to be forgotten"

One of our main conclusions is the need for more transparency in the implementation of the RTBF by private companies. Despite the current lack of this, we had some valuable insight into a data analysis of the practical implementation of the RTBD by Google and "what we currently are forgetting". In spite of the limited sample of the study and the caution we must proceed with in drawing general conclusions from it, we saw that most of the requests for removal analysed in the study were related to some kind of past criminal offense or felony.

Here, we would like to echo the questions we raised earlier, as to whether the "right to be delisted" (or even possibly other variations of the RTBF) could actually be more related to the principle of rehabilitation than initially thought. In this regard, could future reforms of bankruptcy or criminal legislations also have an impact on the right to internet privacy? Should these kinds of reforms also take into consideration a possible "expiry date" or "obscurity" for such information, as is the case now with some criminal registries? To answer these questions, I believe a more in-depth interdisciplinary study of the right to be forgotten is necessary. But, for now, we can at least remember that the internet does not forget.

# BIBLIOGRAPHY


ÁLVAREZ RIGAUDIAS, C. (2014, September 3). Sentencia Google Spain y Derecho al Olvido. *Actualidad jurídica Uría Menéndez /110-118*.

ARTICLE 19. (2014, October 16). *ARTICLE 19's Response to Google's Advisory Council.* Retrieved from https://www.article19.org/data/files/medialibrary/37733/A19-comments-on-RTBF-FINAL.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2014, November 26). Article 29 Data Protection Working Party - PRESS RELEASE - Adoption of guidelines on the implementation of the CJEU's judgement on the "right to be forgotten". Brussels, Belgium. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2014/20141126_wp29_press_release_ecj_de-listing.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2014). *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12.* Brussels: Directorate General Justice of the European Commission.

AUSLOOS, J. (2015, September 18). *CJEU is asked to rule on the 'Right to be Forgotten' again.* Retrieved from KU Leuven Centre for IT & IP Law: https://www.law.kuleuven.be/citip/blog/cjeu-is-asked-to-rule-on-the-right-to-be-forgotten-again/

BERMAN, J. & MULLIGAN, D. (1999). The Internet and the Law: Privacy in the DigitalAge: A Work in Progress. *Nova Law Review. 549, 554*.

BIRD & BIRD. (2017, May). *Bird & Bird guide to the General Data Protection Regulation.* Retrieved from https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en

Camera di Commercio di Lecce v Salvatore Manni, C-398/15 (Court of Justice of the European Union March 9, 2017).

CJEU. (2013, June 25). Press Release No 77/13 (Advocate General's Opinion in Case C-131/12).

DE TERWANGNE, C. (2012, February). Internet Privacy and the Right to Be Forgotten/Right to Oblivion. *Revista de Internet, Derecho y Política*.

DeVRIES, W. T. (2003). Protecting Privacy in the Digital Age,. *18 Berkeley Tech. L.J. 283*, 283-311.

DeVRIES, W. T. (2003). Protecting Privacy in the Digital Age,. *18 Berkeley Tech. L.J. 283*, 283-311.

ECHIKSON, W. (2013, February 26). *Judging freedom of expression at Europe's highest court* . Retrieved from Google Europe Blog: https://europe.googleblog.com/2013/02/judging-freedom-of-expression-at.html

EDWARD LEE. (2015, May 07). *Judge Google: Why the EU Should Embrace Google's Role in the Right to Be Forgotten.* Retrieved from Huffington Post: http://www.huffingtonpost.com/edward-lee/judge-google-why-the-eu-s_b_7232688.html

ERIC SCHMIDT & JARED COHEN. (2014). *The New Digital Age: Transforming Nations, Businesses, and Our Lives.* Vintage Books.

EUROPEAN COMMISSION. (2014). *Factsheet on ECJ's ruling on the 'right to be forgotten' in relation to online search engines.* Retrieved from European Commission. Justice. Data Protection. Documents.: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

EUROPEAN COMMISSION. (2015). *Special Eurobarometer 431: Data Protection.* Retrieved from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf

European Union Committee, HOUSE OF LORDS OF THE UNITED KINGDOM. (2014). *EU Data Protection law: a 'right to be forgotten'?* London. Retrieved from https://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf

FLORIDI, P. L. (2014, July 2014). Prof Luciano Floridi, Professor of Philosophy and Ethics of Information, Oxford Internet Institute, University of Oxford—Written evidence (TRF004). (T. E.-T. Lords, Interviewer)

GOOGLE. (2017, May 25). *European privacy requests for search removals*. Retrieved from Transparency Report: https://www.google.com/transparencyreport/removals/europeprivacy/

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

HARTZOG, W. & STUTZMAN, F. (2013). The Case for Online Obscurity . *California Law Review Vol. 101*.

HARVARD LAW REVIEW. (2014, December). Court of Justice of the European Union creates presumption that Google must remove links to personal data upon request. - Case C-131/12, Google Spain SL v. AEPD (May 13, 2014). Retrieved from https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/

HUSOVEC, M. (2014, May 30). Should We Centralize the Right to Be Forgotten Clearing House? *Center for Internet & Society at Stanford Law School*.

IGLEZAKIS, I. (2016). The Right To Be Forgotten: A New Digital Right for cyberspace. *Segurança da informação e Direito Constitucional do ciberespaço.* Lisbon.

JÄÄSKINEN, N. (2013). *Opinion of Advocate General. Case C-131/12.*

KELLEHER, D. (2017, March 9). *Manni: Does the right to be forgotten apply to company registers?* Retrieved from International Association of Privacy Professionals (IAPP): https://iapp.org/news/a/manni-does-the-right-to-be-forgotten-apply-to-company-registers/

KELLY, C. (2015, April 2015). *Google Spain v AEPD and Mario Costeja González*. Retrieved from https://h2o.law.harvard.edu/collages/34086

MAYER-SCHÖNBERGER, V. (2013, April 3). Right to erasure protects people's freedom to forget the past, says expert. (K. Connolly, Interviewer)

PETER FLEISCHER. (2011, March 09). *Foggy thinking about the right to oblivion*. Retrieved from https://peterfleischer.blogspot.com.es/2011/03/foggy-thinking-about-right-to-oblivion.html

REDING, V. (2012, January 22). *Speech on The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age.* Retrieved from http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

REYMOND, M. (2016, September 15). Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the EU Right to be Delisted. 2016. *Berkman Klein Center: Research Publication No. 2016-12*. Retrieved from

https://poseidon01.ssrn.com/delivery.php?ID=174093090115100077025078089094096027052072023065091036126127068087082109005124001086061123008063054013023106093102076104005002041010074040047006100024076112020031046064063083096004096123080119066064121003080070 0

ROSEN, J. (2012). The Privacy Paradox: Privacy and Its Conflicting Values. The right to be Forgotten. *64 STAN. L. REV. ONLINE*. Retrieved from https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/

SCHWARTZ, P. & SOLOVE, D. (2014). Reconciling Personal Information in the United States and European Union. *California Law Review Vol. 102:877*.

SELINGER, E. & HARTZOG, W. (2014, May 20). *Google Can't Forget You, But It Should Make You Hard to Find.* Retrieved from www.wired.com: https://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/

SELINGER, E. & HARTZOG, W. (2015). Why you Have the Right to Obscurity. *Christian Science Monitor (Apr. 15, 2015)*, http://fw.to/6Hn8C1c. Retrieved from http://fw.to/6Hn8C1c

SOLOVE, D. (2014, May 13). *What Google Must Forget: The EU Ruling on the Right to Be Forgotten.* Retrieved from https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten

THE ECONOMIST - Leaders Section. (2017, May 6). *Regulating the internet giants: The world's most valuable resource is no longer oil, but data.* Retrieved from The Economist: http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valu

THE ECONOMIST. (2014, May 17). On being forgotten. *The Economist*.

THE GUARDIAN - Samuel Gibbs. (2016, February 11). *Google to extend 'right to be forgotten' to all its domains accessed in EU.* Retrieved from The Guardian: https://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom

U.S. Federal Trade Commissioner Julie Brill. (2014). Privacy in the Age of Omniscience: Approaches in the United States and Europe. *Mentor Group Vienna Forum.* Vienna. Retrieved from https://www.ftc.gov/system/files/documents/public_statements/581751/140911mentorgroup.pdf

W. G. VOSS & C. C. RENARD. (2016). *Proposal For An International Taxonomy On The Various Forms Of The "Right To Be Forgotten": A study on the convergence of norms.* Retrieved from http://ctlj.colorado.edu/wp-content/uploads/2016/06/v.3-final-Voss-and-Renard-5.24.16.pdf

WARREN, Samuel D. & BRANDEIS, Louis D. (1890). The Right to Privacy. *Harvard Law Review 193*.

XUE, M., MAGNO, G., CUNHA, E., ALMEIDA, V., & ROSS, K. W. (2016). The Right to be Forgotten in the Media: A Data-Driven Study. *Proceedings on Privacy Enhancing Technologies, 2016 no. 4*, 389-402.

# ANNEX

# 1. Legal framework

## 1.1. Charter of Fundamental Rights of The European Union

Link: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

**Article 7. Respect for private and family life**

Everyone has the right to respect for his or her private and family life, home and communications.

**Article 8. Protection of personal data**

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

**Article 11. Freedom of expression and information.**

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
2. The freedom and pluralism of the media shall be respected.

## 1.2. Directive 95/46 – Data Protection Directive

Link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

**Recital 10 in the Preamble.**

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.

**Recital 25 in the Preamble.**

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

**Article 1. Object of the Directive.**

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

**Article 2. Definitions.**

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(d) 'controller' shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

**Article 3. Scope.**

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

**Article 4. National law applicable.**

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

**Article 6. Principles Relating to Data Quality.**

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with.

**Article 7. Criteria for Making Data Processing Legitimate.**
Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

**Article 9. Processing of personal data and freedom of expression.**
Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

**Article 12. Right of access.**
Member States shall guarantee every data subject the right to obtain from the controller: (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

**Article 14. The data subject's right to object.**

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

## 1.3. Regulation 2016/679 - General Data Protection Regulation

Link: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

**Article 17. Right to erasure ('right to be forgotten').**

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

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

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right

referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

### 1.4. Directive 68/151

Link: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31968L0151

**Article 2. Disclosure.**

1. Member States shall take the measures required to ensure compulsory disclosure by companies of at least the following documents and particulars:

(d) The appointment, termination of office and particulars of the persons who either as a body constituted pursuant to law or as members of any such body:

(i) are authorised to represent the company in dealings with third parties and in legal proceedings;

(ii) take part in the administration, supervision or control of the company.

It must appear from the disclosure whether the persons authorised to represent the company may do so alone or must act jointly;

(j) The appointment of liquidators, particulars concerning them, and their respective powers, unless such powers are expressly and exclusively derived from law or from the statutes of the company;

## 2. Google V. Costeja - CJEU preliminary ruling

### 2.1. The Audiencia Nacional's questions:

1. The territorial application of Directive 95/46:
    a. When does an *establishment* exists under art. 4(1)(a)?
    b. When is there is "*use of equipment* situated on the territory of a Member State" under art. 4(1)(c)?
2. The activity of search engines as providers of content in relation to Directive 95/46:
    a. When information within Google Search's activity as a provider of content contains *personal data* of third parties: must its activity be interpreted as "*processing of data*" under art. 2(b)?
    b. If the answer is affirmative: must it be interpreted as meaning that the undertaking managing Google Search is to be regarded as the "*controller*" of the personal data contained in the web pages that it indexes, under art. 2(d)?
    c. If the answer is affirmative: to protect the rights embodied in arts. 12(b) and 14 (a), can the AEPD directly impose a requirement on Google Search that it withdraw from its indexes links to information published by third parties, without addressing the owner of the web page on which that information is located?

d. If the answer is affirmative: would search engines' obligation to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?

3. Regarding the scope of the right of erasure and/or the right to object, in relation to the "right to be forgotten": must it be considered that the rights to erasure and blocking of data [art. 12(b)] and the right to object [art. 14 (a)], extend to enabling the data subject to address himself to search engines to prevent indexing of the information relating to him personally, even if the information has been lawfully published by third parties?'

## 2.2. The CJEU's preliminary ruling

### 2.2.1. Question 2(a) and (b), concerning the material scope of Directive 95/46

The Court reinstated that the operation of loading personal data on an internet page must be considered as '*processing'* within the meaning of art. 2(b) of Directive 95/46[252]. In the context of the case, the Court identified that the operator of a search engine '*collects'*, 'retrieves', 'records' and 'organises' information within the framework of its indexing programmes, 'stores' it on its servers and 'discloses' and 'makes it available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in art. 2(b) of Directive 95/46, the Court considered that *they must be classified as 'processing' within the meaning of that provision, regardless of types of information being processed*[253]. Furthermore, t*he operations referred to in Article 2(b) of Directive 95/46 must also be classified as processing where they exclusively concern material that has already been published in unaltered form in the media*[254].

As to whether Google Inc., as the operator of a search engine, must be regarded as the *'controller'* in respect of the processing of personal data, the Court interpreted that it *is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data within the framework of that activity* and which must, consequently, be regarded as the '*controller'* in respect of that processing pursuant to art. 2(d)[255].

In this context, the Court identified that the activity of search engines play a decisive role in making data accessible to any internet user[256]. It argued that when users carry out a search of an individual's name, they can obtain a structured overview of the information that can be found on the internet, enabling them to establish a more or less detailed profile of the data

[252] Case C101/01 Lindqvist EU:C:2003:596, paragraph 25
[253] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) 28.
[254] *Id. supra* paragraph 30.
[255] *Id. supra* paragraph 33.
[256] *Id. supra* paragraph 36.

subject[257]. Hence, it concluded that *given that the activity of a search engine is therefore liable to significantly affect the fundamental rights to privacy and to the protection of personal data, the operator of the search engine, as the controller, must ensure that its activity meets the requirements of Directive 95/46*[258].

Hence, regarding Questions 2(a) and (b), the Court declared that arts. 2(b) and (d) of Directive 95/46 are to be interpreted as meaning that *the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data*[259]. Additionally, *the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d)*[260].

### 2.2.2. Question 1(a) to (d), concerning the territorial scope of Directive 95/46.

Some important considerations that the Court took into special account when answering this question were:

- Google Search is operated by Google Inc., which is the parent company of the Google Group and has its seat in the United States.
- Google Search indexes websites throughout the world and takes economic advantage of that activity by including advertising associated with the internet users' search terms.
- Through its subsidiary in Spain [Google Spain], the Google Group promotes the sale of advertising space generated on the website 'www.google.com'. Google Spain possesses separate legal personality and its activities are targeted essentially at undertakings based in Spain, acting as a commercial agent for the Google group. Its objects are to promote, facilitate and effect the sale of on-line advertising products and services to third parties and the marketing of that advertising.
- Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc.
- Google Spain forwards Google Inc. requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to protection of personal data.

[257] *Id. supra* paragraph 37.
[258] *Id. supra* paragraph 38.
[259] *Id. supra* paragraph 41.
[260] In Annex section 1.2. of this dissertation.

In establishing the territorial scope of Directive 95/46, the Court first assessed whether the activity of Google Spain was sufficiently linked to that of its parent company's search engine. The Court found that the promotion and sale of advertising space, which Google Spain attends to in respect of Spain, constitutes the bulk of the Google group's commercial activity and may be regarded as closely linked to Google Search[261]. The Court then proceeded to identify the requirements set out in Recital 19 in the preamble to Directive 95/46 and art. 4(1)(a). Recital 19 in the preamble states that "*establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements*" and that "*the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor*"[262]. To satisfy the criterion laid down in that provision, the Court noted that *it is also necessary that the processing of personal data by the controller be "carried out in the context of the activities' of an establishment of the controller on the territory of a Member State*[263]*"*, under art. 4(1)(a). The Court found that those words cannot be interpreted restrictively[264].

In that regard, the Court held that the processing of personal data for the purposes of the service of a search engine such as Google Search, is carried out "in the context of the activities" of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable[265]. In such circumstances, the activities of the operator of the search engine and those of its Spanish establishment were inextricably linked, since the activities relating to the advertising space constitute the means of rendering the Google Inc.'s search engine economically profitable and that engine is, at the same time, the means enabling those activities to be performed[266].

Hence, regarding Question 1(a), the Court declared that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State[267]. Moreover, in view of the answer given to Question 1(a), the Court found that there was no need to answer Questions 1(b) to (d)[268].

[261] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 46.
[262] *Id. supra* paragraph 48.
[263] *Id. supra* paragraph 50.
[264] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) quoting Case C‑324/09 L'Oréal and Others EU:C:2011:474, paragraphs 62 and 63.
[265] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 55.
[266] *Id. supra* paragraph 56.
[267] *Id. supra* paragraph 60.
[268] *Id. supra* paragraph 61.

### 2.2.3. Question 2(c) and (d), concerning the extent of the responsibility of the operator of a search engine under Directive 95/46

In answering this question, the Court took into special account:

- Art. 1[269] and recital 10 in the preamble[270] to Directive 95/46, which aim to guarantee a high level of protection of natural persons' right to privacy.
- Recital 25[271] in the preamble to Directive 95/46, regarding the principles of protection laid down by the directive through the obligations imposed on persons responsible for processing and the rights conferred on individuals whose data are the subject of processing[272].
- Arts. 7[273] and 8[274] of the Charter regarding the rights to respect for private life and the right to the protection of personal data, respectively.

According to the Court, the notion of "*inaccurate nature of the data*" stated in art. 12(b) of the Directive is related the principles relating to data quality, defined in art. 6[275] of the Directive. The Court understood that the requirements referred to in art. 6(1)(d) of Directive 95/46 were stated by way of example and were not exhaustive. And therefore, *that the non-compliant nature of the processing can confer the rights to rectification, erasure or blocking of data, under art.12(b) of the directive and that such rights may also arise from non-observance of the other conditions of lawfulness regarding the processing of personal data*[276]. In connection to this, the Court reinstated that it had previously established that, subject to the exceptions under art. 13, all processing of personal data must comply both with[277]:

1. the principles relating to data quality set out in art. 6 of the Directive.
2. one of the criteria for making data processing legitimate listed in art. 7[278] of the Directive.

In the context of art. 6 of the Directive, the Court declared that the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified[279].

Regarding legitimation under art. 7 of the Directive, the Court understood that processing carried out by the operator of a search engine, was capable of being covered under Article

[269] In Annex section 1.2. of this dissertation.
[270] *Id. supra.*
[271] *Id. supra.*
[272] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 67.
[273] In Annex section 1.1. of this dissertation.
[274] *Id. supra.*
[275] In Annex section 1.2. of this dissertation.
[276] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 70.
[277] *Id. supra.* paragraph 71.
[278] In Annex section 1.2. of this dissertation.
[279] (Google Spain SL, Google Inc v. Agencia Española de Proteccion de Datos, Mario Costeja González, 2014) paragraph 72.

7(f)[280]. In this regard, it also pointed out that *the wording of Article 7(f) implies that it requires a balancing of the opposing rights and interests concerned, with special account of the data subject's rights arising from Articles 7 and 8 of the EU Charter of Fundamental Rights*[281]. *The data subject may also rely on the right to object laid down in art. 14(a) of the Directive*[282]*, on compelling legitimate grounds relating to his particular situation*. Where there is a justified objection, art. 14(a) states that the processing instigated by the controller may no longer involve those data[283].

The Court proceeded to declare that *requests under articles 12(b) and 14(a) of Directive 95/46 could be addressed by the data subject directly to the controller*. Then, the controller had to examine the merits of the requests on a case-by-case basis, and if justified, end the processing of the data. *Where the controller does not grant the request, the data subject may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly*[284].

In connection to this, the Court insisted on the fact that processing of personal data carried out by the operator of a search engine is liable to significantly affect the fundamental rights to privacy and to the protection of personal data. *When searching an individual's name on a search engine, that processing enables any internet user to obtain information relating to that individual that can be found on the internet, which could potentially concern a vast number of aspects from the data subject's private life. In addition, search engines allow any internet user to establish a more or less detailed profiles of individuals, by obtaining a structured overview of information which could not have been interconnected or could have been only with great difficulty*. Furthermore, the Court also recognised that *the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous* (see, to this effect, Joined Cases C‑509/09 and C‑161/10 eDate Advertising and Others EU:C:2011:685, paragraph 45) [285].

Given the potential seriousness of the interference of processing within the activity of search engines, the Court declared that *it could not be justified by merely the economic interest which the operator of such an engine has in that processing*[286]. However, it also noted that *the removal of links from the list of results could have effects upon the legitimate interest of internet users potentially interested in having access to that information*. The Court observed that in situations such as that at issue in the main proceedings a fair balance should be sought in particular between other legitimate interests and the data subject's fundamental rights under arts. 7 and 8 of the Charter.

[280] *Id. supra.* paragraph 73.
[281] *Id. supra.* paragraph 74.
[282] *Id. supra.* paragraph 75.
[283] *Id. supra.* paragraph 76.
[284] *Id. supra.* paragraph 77.
[285] *Id. supra.* paragraph 80.
[286] *Id. supra.* paragraph 81.

In establishing such balance, the Court stated that "whilst the data subject's rights protected by those articles override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life[287]".

In addition, the Court also stated that in the application of arts. 12(b) and 14(a) of the Directive, the supervisory authority or judicial authority may order the operator of the search engine to remove links to web pages published by third parties containing information relating to a data subject, without a previous or simultaneous request for the removal information from the web page on which they were published[288]. The Court justified this by arguing that the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites[289].

In connection to this, the Court found that the outcome the weighing of the interests under Article 7(f) and Article 14(a) of the Directive may differ depending on whether the processing is carried out by the operator of a search engine or by the publisher of the web page is at issue. As an example, it stated that the publisher of a web page consisting in the publication of information relating to an individual may, in some circumstances, be carried out 'solely for journalistic purposes' under Article 9 of Directive 95/46[290]. In this regard, the legitimate interests justifying the processing may, firstly, be different and, secondly, the consequences of the processing for the data subject, and for his private life, are not necessarily the same[291]. Finally, the Court proceeded to acknowledging that the inclusion in the list of results based on a person's name, of a web page and of the information contained on it relating to that person, is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the sole publication on the web page[292].

Hence, in answering questions 2(c) and (d) the Court declared that arts. 12(b) and 14(a) of Directive 95/46 are to be interpreted as meaning that, when requests under those articles meet their requirements, the operator of a search engine is obliged to remove from the list of results displayed following a search made based on a person's name links to web pages, published by third parties and containing information relating to that person. This is also the case where that name or information is not erased beforehand or simultaneously from those web pages, or the publication on those pages is lawful[293].

[287] *Id. supra.* paragraph 81.
[288] *Id. supra.* paragraph 82.
[289] *Id. supra.* paragraph 84.
[290] *Id. supra.* paragraph 85.
[291] *Id. supra.* paragraph 86.
[292] *Id. supra.* paragraph 87.
[293] *Id. supra.* paragraph 88.

### 2.2.4. Question 3, concerning the scope of the data subject's rights guaranteed by Directive 95/46

The application of Article 12(b) of Directive 95/46 is subject to the condition that the processing of personal data be incompatible with the directive. In this regard, the Court declared that *such incompatibility may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes*[294]. *It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed*[295]. Furthermore, the Court stated that in requests founded under art. 12(b) and art. 14(a) of Directive 95/46, *in each case, the processing of personal data must be authorised under Article 7 for the entire period during which it is carried out*[296].

Finally, the Court made an important remark on the balancing of the rights to respect for private life and right to the protection of personal data, embodied under arts. 7 and 8 of the EU Charter of Fundamental Rights. In this regard, the Court stated that "*the data subject may request that the information in question no longer be made available to the general public by its inclusion in such a list of results. As a general rule, the rights embodied in arts. 7 and 8 of the Charter rights override not only the economic interest of the operator of the search engine, but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question*[297].

Hence, in answering Question 3, the Court declared that arts. 12(b) and 14(a) of Directive 95/46 are to be interpreted meaning that, when applying those provisions, *it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order that the inclusion of the information in question causes prejudice to the data subject*. In the light of the fundamental rights embodied under Articles 7 and 8 of the Charter, *the data*

[294] *Id. supra.* paragraph 92.
[295] *Id. supra.* paragraph 93.
[296] *Id. supra.* paragraph 95.
[297] *Id. supra.* paragraph 97.

*subject may request that the information in question no longer be made available to the general public. Those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question*[298].

[298] *Id. supra.* paragraph 97.