EMORY LAW

Emory International Law Review

Volume 32 | Issue 1

2017

Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation

Stefania Alessi

ETERNAL SUNSHINE: THE RIGHT TO BE FORGOTTEN IN THE EUROPEAN UNION AFTER THE 2016 GENERAL DATA PROTECTION REGULATION

INTRODUCTION

"Blessed are the forgetful, for they get the better even of their blunders."

In the movie "Eternal Sunshine of the Spotless Mind," the couple portrayed by Kate Winslet and Jim Carey seeks to erase all memories of each other when their relationship turns sour. Aside from the Hollywood gimmicks of memory erasure, we all have personal information, memories, and opinions that we wish to keep private. The advent of the Internet made this task more complicated.

The Internet revolutionized the information market by allowing people access to a potentially unlimited amount of information with just a computer and connection.[1] Not only is information on the Internet more accessible, but it is also eternal.[2] Once information is uploaded, the Internet stores it permanently, in what has been called "digital eternity."[3] Hence, when personal information is uploaded online,[4] our most embarrassing or painful moments may acquire lasting significance and haunt our lives.[5] The Internet is an integral part of our lives to collect information, manage finances, socialize, and shop. Thus, it risks infringing upon individuals' right to privacy.

In 2014, the Court of Justice of the European Union recognized the existence of the individual right to be forgotten as part of the right to data protection in the case *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (*Google Spain*).[6] The right to be forgotten (RTBF) is the right of an individual to request search engine providers, such as Google, to

---

[1] Barry M. Leiner et al., *Brief History of the Internet*, INTERNET SOCIETY (2016), http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

[2] *See* Michael Douglas, *Questioning the Right to Be Forgotten*, 40 ALTERNATIVE L.J. 109 (2015).

[3] David Lindsay, *Digital Eternity or Digital Oblivion: Some Difficulties in Conceptualising and Implementing the Right to Be Forgotten*, *in* THE RIGHT TO PRIVACY IN THE LIGHT OF MEDIA CONVERGENCE: PERSPECTIVES FROM THREE CONTINENTS 322, 324 (Dieter Dörr & Russell L. Weaver eds., 2012).

[4] Internet users do not always have control over personal information that ends up on the Internet. Some of us may have discovered there is more information online than we wished or expected.

[5] Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017 (2016).

[6] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014).

remove links to personal information that the individual deems prejudicial to him or wishes to be removed.[7] In May 2016, the European Council and the European Parliament enacted the General Data Protection Regulation (GDPR) to provide a uniform normative framework for the RTBF (also called "right to erasure"[8]) and harmonize data protection across the EU.[9]

Google Spain and the GDPR provoked heated criticism and debate as to whether the RTBF should be protected. Some authors argued that there is no expectation of privacy in personal information online.[10] Others predicted that protection of the RTBF will force search engines to remove contents from the Internet and unduly compress the right of access to information and the freedom of expression.[11] Technology think tanks maintained that the new regulation, while giving EU citizens more control over their personal data, will be burdensome to implement for medium and small businesses, governments, and civil society groups, as it will require them to jump through too many hoops. Namely, the heavy burdens of proof and the high administrative sanctions for breach of data protection may discourage the creation of start-ups and impair scientific research.[12]

In response to the critics, this Comment presents two main arguments.

First, the new normative framework of the RTBF is consistent with the well-established protection of the right to respect for private life recognized and protected in international law by the European Court of Human Rights (ECtHR) under the 1950 European Convention on Human Rights (ECHR).

Second, the GDPR will not harm the right to information because it guides search engines to duly balance the right to data protection and the right to information. Clear guidance for the data controllers will result in greater uniformity of decisions in RTBF claims. Also, the structure of the Internet

---

[7] *Id*. at ¶ 21.

[8] "Right to be forgotten" and "right to erasure" are used as synonyms in the Regulation. For the purpose of this Comment, we will only use the term "right to be forgotten."

[9] Regulation 2016/679, O.J. L 119/1 (2016).

[10] Sanduni Wickramasinghe, *The Oblivious Oblivion: A Critique on The EUCJ's Right to Be Forgotten* 6 (Nov. 25, 2015), https://ssrn.com/abstract=2782746.

[11] Douglas, *supra* note 2, at 110.

[12] Giacomo Fracassi, *#GDPR: Technology Think Thank Criticized New EU Data Regulation*, EU REPORTER (Apr. 15, 2016), https://www.eureporter.co/frontpage/2016/04/15/gdpr-technology-think-thank-criticized-new-eu-data-regulation/.

market will safeguard the right to information and the search engine's economic rights.

This Comment will focus solely on the protection of the RTBF in the EU and will not address issues related to the territorial application of the European data protection legislation.

Part I provides an overview of the regulation of the right to private life, which germinates the right to data protection and the RTBF. Part II describes the evolution of the RTBF, from the Data Protection Directive to the *Google Spain* decision. Part III discusses the new discipline of the RTBF introduced by the 2016 GDPR. Part IV explains that the GDPR is in line with the EU protection of the right to data protection and right to respect for private life and that the GDPR will not harm the right to information.

I. PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

The right to protection of personal data is part of the broader human right to respect for private life,[13] which is recognized and protected both in international law and in EU law.[14] This section analyzes the scope of the right to respect for private life and its evolution, with particular reference to the right to protection of personal data.

A. The International Framework

The right to respect for private life was first recognized as a human right in international law by the ECHR.[15] Article 8 of the ECHR establishes that "everyone has the right to respect for his private and family life, his home and his correspondence."[16] The right is formulated broadly and protects individuals' autonomy and dignity in developing their personalities both privately and in

---

[13] The right to respect for private life may also be treated as a stand-alone human right. *See* Dan Manolescu, *Data Protection as a Fundamental Right*, 5 EFFECTIUS NEWSLETTER 1 (2010).

[14] *Handbook On European Data Protection Law*, EUROPA 1, 14 (2014), http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf [hereinafter *Data Handbook*].

[15] European Convention on Human Rights, Dec. 4, 1950, art. 8. The ECHR was drafted under the auspices of Council of Europe. *Id*. The EU is not part of the Council of Europe, but all the EU Member States are also members of the Council of Europe. *Data Handbook*, *supra* note 14, at 15. The Council of Europe is an international organization headquartered in Strasbourg, France, has 47 member states, and was created to promote democracy and protect human rights in Europe. *Who We Are*, COUNCIL OF EUROPE (2016), http://www.coe.int/en/web/about-us/who-we-are. The EU is an economic and political union headquartered in Brussels, Belgium, has 28 member states, and was created to foster economic cooperation. *The EU in Brief*, EUROPA (2016), https://europa.eu/european-union/about-eu/eu-in-brief_en.

[16] European Convention on Human Rights, *supra* note 15, art. 8.

relationships with others.[17] Hence, the right to respect for private life is broader than the right to privacy because it is not limited to the protection of individuals' intimate spheres but includes the right of individuals to freely pursue and fulfill their personalities in relationships with others.[18] The right to private life is not absolute.[19] Indeed, it can be restricted to achieve legitimate public interests like national security, public order, and prevention of crime.[20] The right to private life can also be restricted to protect other human rights.[21] In particular, the right to data protection must be balanced against the right to freedom of expression.[22]

The ECtHR, created by the ECHR to ensure its observance,[23] held that the right to respect for private life imposes positive and negative obligations on the contracting states.[24] The state has to act affirmatively with measures to ensure respect of the right and must not interfere with a person's private life, home, and correspondence.[25]

The development of information and surveillance technology in the 1960s created the need to protect individuals' private lives by strengthening their personal data protection.[26] Accordingly, a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was opened for signature in 1981.[27] The convention applies to data processing by private and public entities and protects the individuals against abuses in the collection and storage of personal data.[28] Individuals have the right to know that personal information about them is stored and, if necessary, to correct the information. Moreover, the automatic processing and storage of

---

[17] *Article 8 Right to a Private and Family Life*, LIBERTY, https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/article-8-right-private-and-family-life.

[18] Niemietz v. Germany, 80 Eur. Ct. H.R. 29 (1992) ("[I]t would be too restrictive to limit the notion [of private life] to an 'inner circle' in which the individual may live his own personal life as he chooses. . . . Respect for private life must also comprise . . . the right to establish and develop relationships."); Ursula Kilkelly, *The Right to Respect for Private and Family Life*, HUMAN RIGHTS HANDBOOKS NO.1 1, 10 (2003), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007ff47.

[19] *Article 8 Right to a Private and Family Life*, *supra* note 17.

[20] Steven Greer, *The Exceptions to Articles 8 to 11 of the European Convention on Human Rights*, COUNCIL OF EUROPE PUBLISHING 6 (1997), http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf.

[21] *Id.* at 35.

[22] *Article 8 Right to a Private and Family Life*, *supra* note 17.

[23] European Convention on Human Rights, *supra* note 15, art. 19.

[24] Kroon and Others v. Netherlands, App. No. 18535/91, 35 Eur. Ct. H.R. 31 (1994); Kilkelly, *supra* note 18, at 20.

[25] Kilkelly, *supra* note 18, at 20.

[26] *Data Handbook*, *supra* note 14, at 15.

[27] *Id.* at 15–16.

[28] *Id.* at 16.

"sensitive data" (data revealing race, political, religious and other beliefs, health or sexual life) are prohibited.[29] With Convention 108, the Council of Europe aimed to protect individuals' private and family lives against abuses in the automatic collection and storing of personal data introduced by the new information technologies.[30] The convention was the first international instrument to recognize the right to data protection and served as inspiration for the enactment of the 1995 Data Protection Directive by the EU.[31]

B. The European Union Framework

Because the EU was originally conceived solely as an economic union, the founding treaties[32] did not contain any reference to fundamental rights.[33] Nevertheless, since its creation, the European Court of Justice (CJEU) was confronted with fundamental rights issues, especially cases of conflicts between obligations of the Member States and national constitutional laws.[34] The CJEU's jurisprudence gradually filled the gaps of the founding treaties.[35] The development of fundamental rights protection in the EU followed three stages.[36]

In the first stage, the CJEU refused to take on any case that required an examination of European law in terms of fundamental rights and held that the protection of fundamental rights was a matter of exclusive jurisdiction of the Member States.[37] In the second stage, criticism by the Member States and the establishment of the supremacy principle of EU law[38] over national legislation

---

[29] *Id*. at 16; to date, Convention 108 is the only legally binding international instrument in data protection, *Details of Treaty No. 108*, COUNCIL OF EUROPE 1, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[30] *See Details of Treaty No. 108*, COUNCIL OF EUROPE 1, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[31] Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 536/14 (Feb. 2014) at 3.

[32] The Treaty of Paris created the European Coal and Steel Community (ECSC) in 1951. The two Treaties of Rome created the European Economic Community (EEC) and European Atomic Energy Community (EURATOM) in 1957. Finn Laursen, *The Founding Treaties of the European Union and Their Reform*, POLITICS (2016), http://politics.oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-151.

[33] *Data Handbook*, *supra* note 14, at 20; ALINA KACZOROWSKA, EUROPEAN UNION LAW 215 (3rd ed. 2013).

[34] KACZOROWSKA, *supra* note 33, at 215.

[35] *Fundamental Rights in the European Union*, EUROPEAN PARLIAMENT, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf.

[36] KACZOROWSKA, *supra* note 33, at 215.

[37] *See* Case 1/58 *Friedrich Stork & Cir v High Authority* [1959] ECR 17; *see also* KACZOROWSKA, *supra* note 33, at 215.

[38] The supremacy doctrine was developed by the ECJ in a series of important decisions. Under the doctrine, in case of conflict between European Union law and the law of Member States, European Union law

led the CJEU to declare that fundamental rights were general principles of EU law and therefore protected by the CJEU.[39] Finally, in the third stage, the CJEU held that the Member States are also bound by EU fundamental rights when acting within the scope of the EU.[40] The court thus ensured consistent protection of fundamental rights by EU institutions and national governments.[41] However, the EU still lacked its own bill of fundamental rights.

The 1992 Treaty of Maastricht, which formally created the EU, recognized the fundamental rights guaranteed by the ECHR as fundamental principles of EU law.[42] Accordingly, the EU recognized the right to respect for private life. The EU institutions then sought to enhance the protection of these rights by introducing an EU bill of rights. The goal was achieved through the proclamation of the Charter of Fundamental Rights of the European Union (Charter) in 2000.[43]

The Charter brings together the fundamental rights and principles protected in the EU, including the rights recognized by the CJEU, the rights and principles resulting from the common constitutional traditions of the Member States, and the rights and freedoms protected by the ECHR.[44] Although the Charter was originally just a political document, the 2009 Treaty of Lisbon made the Charter binding upon the Member States and the EU institutions.[45]

The Charter guarantees not only the right to respect for private and family life,[46] but also establishes the right to "protection of personal data,"[47] making it a distinct fundamental right in EU law.[48] The right to data protection is the right of individuals (data subjects) to know what, where, and how information about

---

prevails. *Supremacy of EU Law*, EURWORK (May 4, 2011), https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/supremacy-of-eu-law.

[39] Case 29/69 *Erich Stauder v City of Ulm-Sozialamt* [1969] ECR 419; KACZOROWSKA, *supra* note 33, at 214-15, 218.

[40] KACZOROWSKA, *supra* note 33, at 218.

[41] *See generally* EUROPEAN PARLIAMENT, *supra* note 35.

[42] KACZOROWSKA, *supra* note 33, at 221.

[43] Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2001 O.J. C 364 [hereinafter Charter].

[44] *Data Handbook*, *supra* note 14, at 20; KACZOROWSKA, *supra* note 33, at 215.

[45] *Handbook On European Data Protection Law*, EUROPA 1, 20 (2014), http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf; KACZOROWSKA, *supra* note 33, at 214.

[46] Charter, *supra* note 43, art. 7

[47] Charter, *supra* note 43, art. 8.

[48] *Data Handbook*, *supra* note 14, at 20; Opinion of the Article 29 Working Party on the Application of Necessity and Proportionality Concepts and Data Protection Within the Law Enforcement Sector Data Protection Within the Law Enforcement Sector, 2014 O.J. (C 536) at 2–3.

them (personal data) is gathered, stored, transferred, and made public.[49] The enforcement of this right may require the withdrawal of certain personal data from the public domain.[50] In the EU, the right to data protection, as a general rule, trumps economic interests and other interests in making and keeping personal data public.[51] Nevertheless, the right to data protection is not absolute and may be restricted for important public interest reasons, such as the right of the public to access personal information about important public figures.[52]

C. The Principle of Proportionality

Article 52 of the Charter requires any limitations on a fundamental right or freedom guaranteed by the Charter to be adopted by law and subject to the principle of proportionality.[53] The principle originally developed in German administrative law and evolved from the case law of the ECtHR applying Article 8 of the ECHR.[54] Under the principle of proportionality, "the action of the EU must be limited to what is necessary to achieve the objectives of the Treaties;"[55] that is, the action can infringe upon a fundamental right only as much as is necessary to achieve the stated goal.[56] The EU adopted the principle of proportionality of Article 8 of the ECHR and incorporated it in the Charter.[57]

For the proportionality test to apply, an individual must first show that he has a fundamental right and that a governmental action infringes upon that right.[58] If he succeeds, the burden shifts to the government to prove three

---

[49] Dan Manolescu, *Data Protection as a Fundamental Right*, 5 EFFECTIUS NEWSLETTER 1 (2010).

[50] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014).

[51] *Id.* ¶ 81.

[52] In this case, keeping public and accessible personal information in the name of the right to freedom of information might be justifiable. *See, e.g.*, CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, ¶ 48.

[53] Charter, *supra* note 43, art. 52.

[54] Opinion of the Article 29 Working Party on the Application of Necessity and Proportionality Concepts and Data Protection Within the Law Enforcement Sector Data Protection, 2014 O.J. (C 536) at 2–3 [hereinafter *Working Party Opinion*]; Moshe Cohen-Eliya & Iddo Porat, *American Balancing and German Proportionality: The Historical Origins*, 8 INT'L. J. CONST. L., 263, 266 (2010).

[55] *Proportionality Principle*, EURLEX, http://eur-lex.europa.eu/summary/glossary/proportionality.html.

[56] Charter, *supra* note 43, art. 52; PENELOPE KENT, LAW OF THE EUROPEAN UNION 45–46 (Harlow Longman ed., 3rd ed. 2001). Under many aspects, the principle of proportionality resembles the balancing doctrine in the American constitutional system, although the balancing doctrine in not an established doctrine in the American juridical system. Cohen-Eliya & Porat, *supra* note 54, at 265.

[57] *See Working Party Opinion*, *supra* note 54, at 4.

[58] *See* Case C-292/97, Kjell Karlsson and Others, 2000 E.C.R. I-02737; *Fundamental Rights in the European Union*, at 13 (Mar. 27, 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf.

elements: (1) that the limitation is in accordance with the law;[59] (2) that the pursued goal is legitimate; and (3) that the action was necessary to achieve the stated goal.[60] Proportionality is broadly interpreted as part of the necessity element and requires that the stated goal of the restriction cannot be achieved through less restrictive means.[61] If the stated goal of the restriction can be achieved by less restrictive means, and if less restrictive means are available, then the measure is not proportional.[62] The CJEU found that, "in assessing whether processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognized by Art[icles] 7 and 8 of the Charter but will still contribute effectively to the objectives of the EU rules in question."[63]

Although the Charter recognized the right of data protection as a fundamental right and provided a standard for its enforceability,[64] the EU still lacked a thorough legislative regulation of the right to data protection.

II. FROM THE DATA PROTECTION DIRECTIVE OF 1995 TO THE *GOOGLE SPAIN* DECISION: THE RECOGNITION OF THE RIGHT TO BE FORGOTTEN

The EU first regulated the right to data protection with the Data Protection Directive of 1995 (DPD).[65] Twenty years later, in the *Google Spain* case, the CJEU interpreted the DPD to recognize the right to be forgotten (RTBF).[66] This

---

[59] To be in accordance with the law, the governmental activity must be based on domestic law and "be compatible with the rule of law" and must be "adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to regulate his or her conduct." Working Party Opinion, *supra* note 54, at 5.

[60] Working Party Opinion, *supra* note 54, at 5; Cohen-Eliya & Porat, *supra* note 54, at 267.

[61] Working Party Opinion, *supra* note 54, at 12; KENT, *supra* note 56, at 45–46. For example, refusal to withdraw a secretly recorded video of an individual's intimate moments from the public domain would likely be disproportional because the individual right to private life outweighs the right to information. On the other hand, refusal to withdraw from the public domain a video about a famous actor's or a politician's extramarital affair may not be disproportional because the public interest in the information likely outweighs the individual's interest.

[62] *See* Working Party Opinion, *supra* note 54, at 12.

[63] Case C-291/12, Michael Schwarz v. Stadt Bochum, ECLI:EU:C:2013:401 (2013) ¶ 46. The European courts may apply the principle of proportionality to cases involving very different interests and that involve both legislative and administrative acts. Takis Tridimas, *Proportionality in Community Law: Searching for the Appropriate Standard of Scrutiny*, *in* THE PRINCIPLE OF PROPORTIONALITY IN THE LAWS OF EUROPE 67 (Hart Publ. 1999). Accordingly, the intensity of the court's review may vary considerably in consideration, for example, of how strictly the court is willing to apply the test and on how much it is willing to defer to the EU authority's discretion. *Id.*

[64] *See* Tridimas, *supra* note 63, at 67.

[65] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter DPD].

[66] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014).

section provides an overlook of the DPD and the CJEU decision, with particular reference to the evolution of the right to data protection in the face of the advent and development of the Internet.

A. The 1995 Data Protection Directive

The European Parliament and Council enacted the DPD to regulate the free flow of personal data across the EU Member States and to set a baseline of protection for the "fundamental rights and freedoms of natural persons and in particular their right to privacy."[67] The necessity to harmonize the regulation of the right to privacy came from the recently created European Single Market.[68] The EU predicted that free movement of goods, capital, services, and people would cause a substantial increase in cross-border flows of personal data, which required a uniform level of data protection.[69]

The DPD is, as a directive, *sui generis*. Whereas typically European directives provide a broad regulatory goal and leave the Member States wide discretion to determine the time and mode of implementation, the DPD allows only limited freedom of implementation.[70] The EU legislature wanted to harmonize national privacy laws across the Member States without reducing protection.[71]

The DPD regulates the collection and processing of personal data and imposes obligations on data controllers, which are entities that determine the means and purposes of the processing of personal data.[72] Personal data has been defined as, "any information relating to an identified or identifiable natural person."[73] First, States must provide that controllers may collect personal data only for "specified, explicit and legitimate purposes"[74] in a way that is "adequate, relevant and not excessive" with respect to the purpose for which the

---

[67] DPD, *supra* note 65, ¶ 38.

[68] *See id.* ¶ 7.

[69] DPD, *supra* note 65, ¶¶ 5, 7; *Data Handbook*, *supra* note 14, at 17–18.

[70] *Data Handbook*, *supra* note 14, at 18; *see Regulations, Directives and Other Acts*, EUROPEAN UNION (2016), https://europa.eu/european-union/eu-law/legal-acts_en.

[71] *See* DPD, *supra* note 65, ¶ 1.

[72] *Id.* art. 2(d).

[73] *Id.* art. 2(a). Under EU law, personal data is information that either directly identifies an individual or describes an individual in a way which makes it identifiable by conducting further research. *Data Handbook*, *supra* note 14, at 36.

[74] DPD, *supra* note 65, art. 6(1)(b).

data are collected.[75] Second, the Member States must provide that personal data are processed "fairly and lawfully."[76]

Even if the RTBF was not yet born, the DPD contained a "right of rectification" that allowed individuals to obtain rectification, erasure, or blocking of incomplete or inaccurate data.[77] This provision laid down the foundation for the RTBF in the *Google Spain* decision.[78] Finally, the DPD permits controllers to store personal data only during the time necessary to collect and process the data as originally intended.[79] Although the DPD contained traces of the main features of the RTBF, the time was not ripe for its recognition.

B. The Development of the Internet and the New Needs of Data Protection

When the DPD was enacted, the Internet looked nothing like it does today.[80] In 1995, only 0.4% of the world population used the Internet, vis-à-vis fifty percent today.[81] Computers had slower processors and smaller memories, which made online research difficult and time-consuming.[82] Many households did not even have a computer or an Internet connection.[83] Search engines were scarce and undeveloped.[84] For example, the Yahoo.com domain was registered in January 1995, only a few months before the directive's enactment.[85] Google did not exist.[86] In the late 1990s, the amount of content available online increased

---

[75] *Id.* art. 6(1)(c).

[76] *Id.* art. 6(1)(a).

[77] *Id.* art. 6(1)(d); Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017, 1028 (2016).

[78] Lee, *supra* note 77, at 1028.

[79] DPD, *supra* note 65, art. 6(1)(e).

[80] In the *Google Spain* case, Advocate General Jääskinen pointed out: "[When] the Directive was adopted in 1995 the internet had barely begun and . . . rudimentary search engines started to appear. . . . Nowadays almost anyone with a smartphone or a computer could be considered to be engaged in activities . . . to which the Directive could potentially apply." Opinion of Advocate General Jääskinen ¶ 10, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014); Lee, *supra* note 77, at 1029.

[81] *Internet Growth Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/emarketing.htm.

[82] *Cf. Comparing Today's Computers to 1995's*, RELATIVELY INTERESTING (Feb. 23, 2012), http://www.relativelyinteresting.com/comparing-todays-computers-to-1995s/ (discussing the "mind boggling" advancements made in the Internet browsing experience).

[83] *Id.*

[84] *See generally* Tom Seymour et al., 15 INT'L J. MGM'T & INFO. SYS. 47, 48 (2011).

[85] *Computer History—1995*, COMPUTER HOPE, http://www.computerhope.com/history/1995.htm (last visited Sept. 6, 2017).

[86] The Google.com domain was registered on September 15, 1997, by Larry Page and Sergey Brinand. The company was incorporated on September 4, 1998, and was based in the garage of a friend (Susan Wojcicki)

exponentially as evidenced by the number of websites growing from approximately 3,000 in 1994 to more than 1 billion in 2014 (a *thirty-three million percent* increase).[87]

The growth of online content and use of the Internet generated a permanent database of personal information.[88] Because servers have an almost unlimited capacity, virtually all information uploaded online is automatically stored as a default procedure.[89] The Internet has made information not only accessible but also eternal.

The Internet's capacity to store information indefinitely was in tension with the text of the Directive, especially where the Directive provided that controllers could store personal data "for no longer than is necessary for the purposes for which the data were collected or . . . processed."[90] That tension remained for almost twenty years until the issue was presented to the European Court of Justice in the *Google Spain* decision.

C. Google Spain *and the Recognition of the Right to be Forgotten*

In 2014, the CJEU faced the issue of applying the DPD to the Internet when the Spanish High Court asked for the interpretation of the DPD and its application to search engines.[91] The questions arose from a 2010 case of Mario Costeja González, a Spanish citizen, against a Spanish newspaper, Google Spain, and Google Inc. for infringement of his privacy rights.[92]

1. The Agencia Española de Protección de Datos

In March 2010, Costeja lodged a complaint with the Agencia Española de Protección de Datos (AEPD), the Spanish data protection agency that administers the DPD in Spain.[93] Costeja alleged that a Google search of his name would return links to two articles of a widely-sold newspaper, where Costeja's

in Menlo Park. *Our History in Depth*, GOOGLE, https://www.google.com/about/company/history/ (last visited Sept. 6, 2017).

87 *Total Number of Websites*, INTERNET LIVE STATS, http://www.internetlivestats.com/total-number-of-websites/ (last visited Sept. 6, 2017).

88 *See* Daniel J. Solove, *Privacy and Power–Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1412 (2001).

89 Lee, *supra* note 77, at 1029.

90 DPD, *supra* note 65, art.12.

91 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014) ¶¶ 18–20.

92 *Id.* ¶ 14.

93 *Id.*

house appeared for a real estate auction in connection with attachment proceedings for the recovery of his debts.[94] Those facts and articles dated back twelve years.[95]

Costeja contended that the publication of that information violated his right to privacy under the DPD because the matter had been resolved and the news was entirely irrelevant.[96] He asked the AEPD to order the newspaper to remove or alter the articles so that his name no longer appeared and to order Google to remove links to the pages from the search results for Costeja's name.[97]

The AEPD denied Costeja's complaint against the newspaper but ruled in his favor against Google. The agency found that the newspaper had no obligation to remove the information contained in the announcements because the announcements had been lawfully published.[98] On the other hand, the agency concluded that Google—and search engines in general—was a data controller subject to the DPD and, upon the individual's request, had the obligation to remove links to personal data that may violate the individual's dignity and fundamental rights to data protection.[99] The agency interpreted the individual rights broadly to include the mere wish of the person that such data would not become known to third parties.[100] To comply with the decision, Google had to conceal the data concerning Costeja by removing the link to the information without having to erase the information itself from the website.[101]

Google Spain and Google Inc. appealed to the Spanish high court, which referred the question of the proper interpretation of the DPD to the CJEU for a preliminary ruling.[102]

2. *The Court of Justice of the European Union*

The CJEU's decision was consistent with the AEPD's interpretation of the Data Protection Directive.[103] Before analyzing if any obligation may attach to Google, the CJEU addressed two preliminary issues: (1) whether search engines fell within the definition of "data controller" of the DPD; and (2) whether the

---

94 *Id.*
95 *Id.*
96 *Id.* ¶ 15.
97 *Id.*
98 *Id.* ¶ 16.
99 *Id.* ¶ 17.
100 *Id.*
101 *See id.*
102 *Id.* ¶¶ 18–20.
103 *See* Lee, *supra* note 77, at 1031.

DPD applied to Google even if Google is headquartered outside EU territory. The court answered both questions in the affirmative.[104]

The Court found that search engines are data controllers because, by indexing information, they disseminate information that would not have been otherwise easily reachable.[105] An Internet search of a person's name, for example, returns a collection of results that together creates a "more or less detailed profile of the data subject."[106] Search engines also process personal data because they collect, record, and store data on their servers to disclose it and make it available to users in the form of search results.[107] Because all of these activities fall within the directive's definition of "processing of personal data,"[108] Google must comply with the DPD.[109]

In addition, the Court held that Google is subject to the territorial application of the DPD. Although Google Inc.—the parent company that operates Google Search—is incorporated in the United States, its subsidiary Google Spain acted as a commercial agent for the Google group in Spain, where it sold and marketed advertising space on "www.google.com."[110] Because the sale of advertising space associated with the user's search terms is the main source of revenue for search engines operators, the court concluded that Google Spain's activity was "inextricably linked" to Google Inc.'s data processing activity.[111] Accordingly,

---

[104] *Google Spain SL v. Agencia Española de Protección de Datos: Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request*, HARV. L. REV. 735, 736–38 (2014), http://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/; *The CJEU's Google Spain Judgment: Failing to Balance Privacy and Freedom of Expression*, EU LAW ANALYSIS (May 13, 2014), http://eulawanalysis.blogspot.com/2014/05/the-cjeus-google-spain-judgment-failing.html.

[105] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014) ¶¶ 17, 100.

[106] *Id.* ¶ 37; *see* Elena Perotti, *The European Ruling on the Right to Be Forgotten and Its Extra-EU Implementation* 11 (Dec. 14, 2015), https://ssrn.com/abstract=2703325 or http://dx.doi.org/10.2139/ssrn.2703325.

[107] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014) ¶ 28.

[108] DPD, *supra* note 65, art. 2(b).

[109] The CJEU found it irrelevant that search engines carry out the same activities with respect of other kinds of information and without affecting a selection between personal data and other information. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014) ¶ ¶ 21, 28.

[110] The court described the market structure of the Internet and the role of Google Search and other search engines, which not only provide access to content hosted on the indexed websites, but also sells advertising associated with the Internet users' search terms. *Id.* ¶ 43.

[111] *Id.* ¶ 55. The DPD only requires that the processing of personal data be carried out "in the context of the activities" of a company, not necessarily by the company itself. *Id.* ¶ 52.

Google Inc. was sufficiently present in the EU territory to be subject to the DPD.[112]

The broad scope of the rule was the result of a teleological reading of the DPD. The Court reasoned that because the EU legislature intended to provide effective privacy protection, an extensive interpretation of the directive was necessary.[113] Thus, the decision opened the doors to RTBF claims against data controllers based outside of the EU.

The Court then turned to the issue of determining search engines' obligations[114] and held that individuals have the right to obtain the rectification, erasure, or blockage of data which is incomplete or inaccurate from search engines.[115]

The Court considered that the DPD implements Articles 7 and 8 of the EU Charter of Fundamental Rights, which protects the right to private life and the right to privacy of personal data, and concluded that the protection of those rights encompasses the "right to be forgotten."[116] Those rights allow individuals to request that search engines remove links to search results containing personal information.[117] Therefore, the Court established a presumption that the individual right to privacy trumps the general public's right to access information as well as the economic interest of the search engine.[118]

The presumption can be overcome only if, given the identity of the individual, there is a "preponderant interest of the general public in having . . . access to the information."[119] Otherwise, individuals can request the removal of links to web content containing personal information that is either "inadequate, irrelevant or excessive in relation to the purposes of the processing," "not kept up to date," or "kept for longer than is necessary."[120] The search engines' obligation to de-link personal information exists independently

---

112 *Id.* ¶¶ 55–56, 60.

113 *Id.* ¶ 54.

114 *Google Spain SL v. Agencia Española de Protección de Datos: Court of Justice of the European Union Creates Presumption that Google Must Remove Links to Personal Data upon Request*, *supra* note 104.

115 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014) ¶¶ 70, 88.

116 *Id.* ¶ 1; the Court did not use that term beyond that reference. Lee, *supra* note 77, at 1031.

117 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014) ¶¶ 81, 97.

118 *Id.*

119 *Id.* ¶ 97. For example, if the person is a public figure and there is a general public interest in the information.

120 *Id.* ¶ 92.

from a similar obligation directed to the publisher, so even if the information is true and has been lawfully published, like in the Costeja's case, the search engine must remove it if the publication of the personal information infringes upon a data subject's privacy.[121]

3. Critiques to the Google Spain Decision

The Google Spain decision is a landmark decision for data protection in the EU and sets the basis for users' rights on the Internet. Despite that, the vagueness of the decision has attracted some criticism.[122] Although the CJEU claimed to establish a rule that the right to privacy trumps the right to information and the search engine's economic interest, it also required balancing those rights and interests in light of the principle of proportionality.[123] Namely, requests to delete personal information must be assessed on a case-by-case basis taking into account the accuracy, adequacy, and relevance of the information compared to the purposes of the data processing.[124]

In *Google Spain*, the CJEU did not indicate how to apply this principle or how to strike this balance. Namely, it did not explain why Costeja's information had to be removed, whether because it was sixteen years old, it was embarrassing, or the matter had been resolved. In fact, the Court clarified the recognition of the RTBF is not conditioned upon the existence of prejudice to the data subject.[125] So, the Court seemed to suggest a case-by-case approach in the resolution of RTBF claims.[126]

The decision is also unclear as to who should strike the balance.[127] It is possible that the CJEU has placed the onus on search engines to balance the right to privacy and the right to information.[128] Because individuals have direct

---

[121] The CJEU specified that the exception Directive regarding "the processing of personal data carried out solely for journalistic purposes" and "necessary to reconcile the right to privacy with the rules governing freedom of expression" did not apply to search engines. *Id.* ¶ 85.

[122] Perotti, *supra* note 106, at 11–12; Lee, *supra* note 77, at 1033.

[123] Lee, *supra* note 77, at 1034.

[124] *Factsheet on "The Right to be Forgotten Ruling,"* 6 EUR. COMM'N, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (last visited Sept. 6, 2017) ("[C]riteria for accuracy and relevance . . . may critically depend on how much time has passed since the original references to a person. While some search results . . . may remain relevant even after a considerable passage of time, others will not be so, and an individual may legitimately ask to have them deleted.").

[125] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) ('Costeja'), 2014 EUR-Lex 62012CJ0131, ¶ 17 (May 13, 2014) ¶ 96.

[126] *Id.*; Lee, *supra* note 77, at 1034.

[127] *Compare* Douglas, *supra* note 2, at 110, *with* Perotti, *supra* note 106, at 11–12.

[127] Douglas, *supra* note 2, at 109.

[128] *Compare* Douglas, *supra* note 2, at 109–10, *with* Perotti, *supra* note 106, at 11–12.

recourse to the search engine providers to request the de-linking of information, corporations may be called to balance fundamental rights. This interpretation raises concerns that the economic interest of the corporation may not align with the individual interest in data protection.[129] In other words, the interest of search engine providers is to produce and maximize their shareholders' profits.[130] To minimize the risk of litigation and costs, search engine providers may grant every request to be forgotten and consequentially limit the information available online.[131]

After the decision, Google and other search engine providers adopted a more proactive role in the de-linking of information to prevent themselves from being sued.[132] They established internal procedures and guidelines to handle RTBF claims.[133] Nevertheless, the lack of an established formula to strike the balance between the right to data protection and the right to freedom of information may be reflected in conflicting decisions in the adjudication of RTBF claims. Whereas a search engine provider may accept a request to be forgotten, another may consider different elements and reject the same claim.

4. Examples of Other Cases

Despite the critiques, the recognition of the RTBF has proven to be in line with the European Union's protective approach to the individual right to privacy. In the 2014 case *Digital Rights Ireland*, the CJEU applied a proportionality test to strike down a European directive that allowed retention of data from fixed, mobile, or Internet telephony, as well as e-mail communications from six months to two years.[134] The Court balanced the compression of the right to personal data protection with the public interest to security and, even if the interference in the right to privacy could be justified by a general interest to prevent crime and facilitate investigations,[135] the Court held the interference was

---

[129] Douglas, *supra* note 2, at 109.

[130] *Id.*

[131] *Id.* at 109. The decision could address the referring tribunal, the Spanish High Court, which had requested the court's interpretation of the DPD. Under this interpretation, judicial bodies must strike the balance between fundamental rights. Perotti, *supra* note 106, at 11–12.

[132] *See* Lee, *supra* note 77, at 1017, 1044.

[133] *See id*.

[134] Joined Cases C-293 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, 2014 ECR I-238; DPD *supra* note 65 ¶¶ 5–6.

[135] The enactment of the directive was prompted by the terrorist attacks in Madrid in 2004 and in London in 2005. *See* Francesca Bignami, *Protecting Privacy against the Police in the European Union: The Data Retention Directive*, 8 CHI. J. INT'L L. 233, (2007); Mira Burri & Rahel Schär, *The Reform of the EU Data*

too extensive and too dangerous.[136] Moreover, the scope of the state's intrusion on the right to privacy was not proportional to its objectives, and the norms regulating the collection and retention of data were too imprecise.[137] Therefore, the CJEU invalidated the directive because it violated Articles 7 and 8 of the EU Charter of Fundamental Rights.[138]

In 2015, the CJEU affirmed the protection of the right to data protection of European citizens in the cross-border setting when it overturned a Commission decision creating a safe harbor for data protection between the EU and the United States. The Commission's decision aimed to provide uniform protection for personal data transfers across countries' borders.[139] The decision also instructed the European Commission to determine whether a country ensured an adequate level of protection for the transfer of data; that is, equivalent to the fundamental rights and freedoms guaranteed within the EU.[140] An Austrian citizen sued the Irish supervisory authority (the Data Protection Commissioner) because it refused to investigate his complaint that Facebook Ireland's practice of transferring and storing user data in the United States violated his rights to privacy.[141] Examining the level of protection of personal data, the Court found that the American legislation failed the proportionality test for three reasons: (1) it allowed unrestricted storage of personal information transferred from the EU to the United States, without any "differentiation, limitation or exception" based on the objective of collection and storage;[142] (2) it failed to provide an objective criterion to limit public authorities' access to and use of the data;[143] and (3) it failed to provide legal remedies for individuals to access their personal data or

Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-driven Economy, 6 J. INFO. POL'Y 479, 484 (2016).

136 Joined Cases C-293 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, 2014 ECR I-238 ¶ 44.

137 *Id.* ¶ 64.

138 *Id.*

139 The safe harbor scheme provides a series of principles for the protection of personal data to which United States' undertakings may subscribe on a voluntary basis. Commission Decision 2000/520, 2000 O.J. (L 215/7).

140 *Id.*

141 C-362/14, Maximillian Schrems v. Data Protection Commissioner 2015, ECLI: EU:C:2015:650, ¶ 2.

142 *Id.* ¶ 93.

143 *Id.*

to obtain rectification or erasure of that data.[144] Thus, the Court invalidated the Safe Harbor Decision because it violated the Data Protection Directive.[145]

The three CJE decisions above emphasize that, although the Court consistently applied the proportionality test to data protection, the EU data protection framework was inconsistent and fragmentary across the Member States, posing a risk of unequal protection of EU citizens. The EU legislature needed a uniform procedural and substantive regulation of the RTBF. The next section examines the changes introduced by the 2016 General Data Protection Regulation and its effects on the RTBF.

III. THE "RIGHT TO ERASURE" AND THE GDPR DIRECTIVE OF 2016

With an outdated, non-self-executing legislative document and a few judicial decisions defining and protecting the RTBF, the EU needed a sweeping reform to keep up with the recent technological advances and harmonize data protection. Accordingly, in 2015 the EU Commission announced the Digital Single Market Strategy to tear down "regulatory walls" among the Member States and project them in the digital age.[146] As part of that strategy, in April 2016, the European Parliament and Council enacted the General Data Protection Regulation (GDPR), which replaced the DPD.[147] With the GPDR, the EU legislature chose a different regulatory instrument: a regulation instead of a directive. This choice is symptomatic of the legislature's will to reach greater and faster implementation and uniformity. Unlike directives, regulations are self-executing and do not require domestic implementation by the Member States.[148] Regulations immediately become part of the national legal system and

---

144 *Id.* ¶ 98 ("In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter").

145 *Id.*

146 *Commission Communication for a Digital Single Market Strategy for Europe*, at 1, COM (2015) 192 final (May 6, 2015).

147 Council Regulation 2016/679, 2016 O.J. (L 119/1) [hereinafter GDPR]. The Regulation entered into force on May 24, 2016, and will be effective as of May 25, 2018. The GDPR is part of a broader Digital Data Reform, which also includes a directive for the police and criminal justice sector. Directive 2016/680 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data. Similar to the Regulation, the directive entered into force on May 5, 2016, and will be effective as of May 6, 2018. *Reform of the EU Data Protection Rules*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

148 *See Regulations, Directives and Other Acts*, EUROPEAN UNION (2016), https://europa.eu/european-union/law/legal-acts_en.

supersede contrary national laws.[149] The GDPR seeks to clarify and harmonize data protection.[150] Particularly, it grants an unprecedented level of "data sovereignty," meaning that data are subject to EU laws if processed in a Member State, independently from where they are collected.[151] The RTBF—now also called "right to erasure"[152]—is one of the regulation's main focuses. This section highlights the salient features of the RTBF protection, compares the new regulation with the DPD, and exposes some critiques to the regulation.

A. The Right to Be Forgotten in the GDPR

The GDPR provides that individuals have the right to obtain the prompt erasure of personal data from search engines when: (1) the information is no longer necessary in relation to the purposes for which it was collected or processed; (2) the individual withdrew consent or objected to the processing and there are no "legitimate grounds for the processing;" or (3) the personal data have been unlawfully processed.[153] Similar to the RTBF in *Google Spain*, the retention of personal data is lawful when necessary for: (1) exercising the right of freedom of expression and information, (2) complying with a legal obligation, (3) defending legal claims, or (4) achieving public interest purposes in the areas of public health, scientific and historical research, or statistics.[154]

Although the RTBF's limitations are similar to the ones established in *Google Spain*, its protection is strengthened by the fact that, if a controller is obligated to erase personal data that it made public, it must take reasonable steps to inform other controllers who also published the personal data to erase any link

---

149 Burri & Schär, *supra* note 135, at 489.

150 *See How Will The EU's Data Protection Reform Strengthen the Internal Market?*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/files/4_strenghten_2016_en.pdf.

151 GDPR, *supra* note 147, art. 3; *see* Quentyn Taylor, *Border Control: The Age of Data Sovereignty*, INFOSECURITY EUR. (May 27, 2016), http://blogs.infosecurityeurope.com/border-control-the-age-of-data-sovereignty/.

152 GDPR, *supra* note 147, art. 17.

153 *Id.* ("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).").

154 *Id.* preamble 65, art. 7(3).

to or copies of it.[155] This provision targets an issue that *Google Spain* left unresolved. Although Costeja's RTBF claim succeeded against Google, it was unclear whether other search engines would comply with the decision, as the same link may have appeared on Yahoo or Bing. Under the GDPR provision, there will likely be broader protection for individuals because other controllers will be notified that the individual has a valid claim to be forgotten. The controllers may then remove the link as a pre-emptive strategy to avoid being sued themselves, which will ensure a more uniform application of the GDPR. Therefore, the GDPR guides search engines to duly balance the right to privacy and the right to information, and more guidance for the data controllers will result in greater uniformity of decision in RTBF claims.[156]

Additionally, if individuals do not meet the requirements to obtain erasure, they can require controllers to restrict the information. Namely, individuals can compel controllers to obtain consent to further process the information if: (1) they contest the accuracy of data, (2) the processing is unlawful, (3) the controllers no longer need the personal data, or (4) they objected to the existence of a public or legitimate interest to the processing of the data.[157] If the restriction is granted, the controllers can use these individuals' personal data only for storage purposes, unless there are important public interest reasons or if the information is necessary to protect the rights of another legal or natural person.[158]

B. The Obligations on Controllers and Processors

In addition to providing more protection for Internet users, the GDPR also imposes more stringent obligations on data intermediaries. The DPD identified two categories of intermediaries: controllers and processors. Controllers are entities that "determin[e] the purpose and means of the processing of personal data," whereas processors are entities that process (that is, collect, record, organize, or otherwise use) the personal data on behalf of the controller.[159] However, only data controllers were subject to obligations.[160] This aspect was heavily criticized because the advent of search engines and social networks

---

[155] *Id.* art. 17(1). Controllers are entities that define the purpose and ways of processing personal data. *See infra* Part III.B.

[156] If the search engines do not remove the link, the data subject may file a complaint against them. The court would apply the proportionality test to determine whether deletion of the link is an appropriate measure to protect the subject's right to privacy.

[157] *Id.* art. 18(1).

[158] *Id.* art. 18(2).

[159] *Id.* art. 1(1), 2(2d), 2(2e).

[160] Burri & Schär, *supra* note 135, at 494.

advanced processing rapidly, making it difficult to distinguish between controllers and processors.[161] Consequently, data intermediaries could easily elude the data protection provisions.[162]

The GDPR maintains these two categories but imposes obligations on both.[163] Under the new discipline, processors have an independent obligation to ensure the security of personal data.[164] For example, processors must ensure compliance with the GDPR to be appointed by controllers.[165] Accordingly, processors must report all information necessary to demonstrate compliance with the regulation and permit audits conducted by the controller.[166] When processing personal data, processors must follow controllers' written instructions and impose confidentiality obligations on all personnel who process the data.[167]

Controllers' obligations under the GDPR are more stringent than under the DPD. For example, controllers must provide data protection "by design or default," meaning that they must ensure maximum privacy protection as a baseline.[168] To do so, controllers must process personal data limited to the specific purpose for which they were processed.[169] This obligation impinges on the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. Privacy by default applies the principle of proportionality because it safeguards a minimal invasion of the right to privacy.

Moreover, the GDPR imposes heavier burdens of proof compared to the DPD. First, controllers must prove they obtained the individual's consent to the processing of personal data.[170] Second, if the individual objects to the processing of data, the controller must demonstrate "compelling legitimate grounds . . . which override the interests, rights and freedoms of the data subject" to justify the processing of personal data and keep the information online.[171] Therefore, some authors argued that the GDPR makes it easier to object to online

---

161 Colette Cuijpers, Nadezhda Purtova & Eleni Kosta, *Data Protection Reform and the Internet: The Draft Data Protection Regulation*, Tillburg Law School Legal Studies Research Paper Series 1, 6 (2014).

162 *Id.*

163 GDPR, *supra* note 147, art. 4(7), 4(8); Burri & Schär, *supra* note 135, at 494.

164 Burri & Schär, *supra* note 135, at 494.

165 GDPR, supra note 147, art. 28.

166 *Id.*

167 *Id.*

168 *Id.* art. 25.

169 *Id.*

170 *Id.* art. 7.

171 *Id.* art. 21(1).

information and have it removed because providing proof of consent and, especially, of compelling legitimate grounds may be time- and resource-consuming for the controller.[172]

Finally, unlike the DPD, the GDPR provides for heavy administrative sanctions. For infringement of the RTBF, controllers and processors could be fined up to €20 million or up to four percent of their total worldwide annual turnover of the preceding financial year.[173]

IV. THE CONTEXT OF THE GDPR AND ITS IMPLICATIONS

There is a concern that the GDPR may be burdensome to implement because it requires data controllers and processors to jump through too many hoops. Namely, the heavy burdens of proof and the high administrative fines for breach of the right to data protection may discourage the creation of start-ups and impair scientific research.[174] These critics, however, fail to consider two points. First, that the new normative framework of the RTBF is consistent with the well-established protection of the right to respect for private life recognized and protected in international law by the ECtHR. Second, that the GDPR will not harm the right to information because the Internet market structure will safeguard the right to information and the search engine's economic rights.

A. The GDPR Follows Well Established Standards in International Law by the European Court of Human Rights

The GDPR is consistent with the judicial practices of the European Court of Human Rights and the European Convention on Human Rights. As seen in Part I, the protection of human rights in the international community and in the EU is interconnected. Since its creation, the EU has recognized the fundamental rights in the ECHR as fundamental principles of EU law, including the right to data protection.[175] The Charter of Fundamental Rights includes the rights and freedoms protected by the ECHR.[176] Particularly, the right to protection for private life in Article 7 of the Charter corresponds to the one guaranteed in

---

[172] Christine Prorok, *"The Right to be Forgotten" in the EU's General Data Protection Regulation*, MICH. J. INT'L. L. (Mar. 10, 2016), http://www.mjilonline.org/the-right-to-be-forgotten-in-the-eus-general-data-protection-regulation/.

[173] GDPR, *supra* note 147, art 82(5)(c).

[174] *See* Fracassi, *supra* note 12.

[175] KACZOROWSKA, *supra* note 33, at 221.

[176] *Data Handbook*, *supra* note 14, at 20; KACZOROWSKA, *supra* note 33, at 215.

Article 8 of the ECHR,[177] and when the Charter contains rights that correspond to the ECHR, "the meaning and scope of those rights [are] the same."[178]

Because the fundamental rights protected by the ECtHR are also applicable to the Member States, the ECJ established a close dialogue with the Strasbourg court and drew from its judicial practice.[179] The GDPR, and the DPD before it, are in line with the international law standards that prioritize the protection of fundamental rights over economic interests.[180]

Nevertheless, the GDPR has been criticized for providing a level of protection that is still too general because the list of justifications for retaining personal data in the public domain is too open and broad.[181] These critiques fail to consider that a narrow discipline of data protection would ultimately jeopardize the effectiveness of the protection. The GDPR should not provide too much detail because a narrow focus on data protection would disregard the complexity of balancing conflicting interests and applying the proportionality principle, which are part of European legal traditions.[182]

Hence, the EU should continue to develop and interpret the GDPR through judicial practice, as past experience has shown that an exceedingly detailed definition of a right may impair its effective protection. When the European Commission and Parliament enacted the directives against discrimination, they provided a closed list of grounds of discrimination. This list includes discrimination based on racial or ethnic origin,[183] religion, beliefs, disability, age, and sexual orientation.[184] The directives soon proved insufficient to grant effective protection against discrimination not covered by the directives. For example, with respect to gender discrimination, the number of CJEU judgments that discuss the directives is marginal compared to the high number of

---

177 *Explanations Relating to the Charter of Fundamental Rights*, 2007 O.J. (C 303).

178 Charter, *supra* note 43, art. 52(3).

179 *Fundamental Rights in the European Union*, *supra* note 35, at 13.

180 *See* Magdalena Jozwiak, *Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union*, 23 MAASTRICHT J. 404, 408 (2016), http://www.maastrichtjournal.eu/pdf_file/ITS/MJ_23_03_0404.pdf.

181 *See generally Position on the Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, EUR. DIGITAL RIGHTS, https://edri.org/files/1012EDRi_full_position.pdf.

182 Aurelia Tamò & Damian George, *Oblivion, Erasure, and Forgetting in the Digital Age*, J. INTELL. PROP., INFO. TECH. & E-COM., 71 (2014), http://www.jipitec.eu/issues/jipitec-5-2-2014/3997/oblivion,%20erasure%20and%20forgetting%20in%20the%20digital%20age.pdf.

183 Council Directive 2000/43/EC, art. 2(2)(a), 2000 O.J. (L 180) 22, 24.

184 Council Directive 2000/78/EC, art. 2(2)(b), 2000 O.J. (L 303) 16, 19.

decisions.[185] In addition, the implementation of the DPD demonstrates that the Internet develops too fast to warrant a detailed definition.

Moreover, the international legal system offers auxiliary tools to interpret and apply the GDPR. Because the data protections in both the international legal system and the EU legal systems are interconnected, the CJEU can rely on the ECtHR jurisprudence when interpreting the GDPR.

B. Two-Sided Markets and Network Effects

The GDPR may make enforcement of the RTBF difficult for search engines. The enhanced burden of proof and the possibility of being hit with high penalties may bring search engines to grant every request of erasure, thereby jeopardizing the right to information.[186]

However, the Internet market structure suggests that the GDPR will not hinder the right to information and that the market will find an equilibrium between the right to privacy and the right to information.

The Internet is a two-sided market; that is, a market where platforms connect and enable interactions between two or more groups of users.[187] These platforms try to attract and charge each side in an attempt to produce value.[188] For example, video game platforms like Sony PlayStation or Microsoft Xbox try to attract gamers in an effort to induce game developers to work for their platforms. At the same time, these platforms also need these developers to create games which induce gamers to buy their console.[189]

Two-sided markets create "network effects" because the greater the number of users, the more benefits the group receives.[190] For example, if a newspaper publishes fewer news stories, the readers will buy their newspaper from another publisher. As a result, advertising companies who publish their ads on the

---

[185] Thien Uyen Do, *2011: A Case Odyssey into 10 Years of Anti-Discrimination Law*, 12 EU ANTI-DISCRIMINATION L. REV. 1, 11 (2011), http://ec.europa.eu/justice/discrimination/files/antidiscrimination_law_review_12_en.pdf.

[186] *See* Douglas, *supra* note 2, at 109.

[187] Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: An Overview*, MIT 1, 2 (2004), http://web.mit.edu/14.271/www/rochet_tirole.pdf.

[188] *Id.*

[189] *Id.*

[190] *See* Thomas R. Eisenmann, Geoffrey G. Parker & Marshall W. Van Alstyne, *Strategies for Two-Sided Markets*, HARV. BUS. REV. (Oct. 2006), *available at* https://hbr.org/2006/10/strategies-for-two-sided-markets.

newspaper will also walk away because their profits depend on how many readers buy the newspaper.[191]

In the Internet market, search engines are the platforms that connect Internet users on one side with Internet content providers on the other side.[192] The network effects will give search engines the economic incentives to balance the right to privacy and the right to freedom of information and prevent them from removing too much information from the Internet.

Like in the newspaper example, if search engines grant all the requests to be forgotten irrespective of their merits, the information available on the platform will diminish. Users will start leaving the platform to find information on another search engine, and the content providers will eventually leave the platform as well because the loss of users causes the platform to lose value. On the other hand, if the search engines do not grant any requests to be forgotten, they will likely face high litigation costs and suffer reputational harm.[193]

In addition, the right to obtain removal of information only applies to the link to personal information and not to the information itself.[194] Accordingly, when the search engine strikes the balance in favor of the right to privacy, the right to freedom of information is not completely suppressed because the search engine can only remove the link to the information from its platform, not from the Internet as a whole. Internet users can potentially still access that same information through other search engines.

Finally, the GDPR only applies to the EU. Even if a user obtains the removal of private information from one of Google's European domains, the information can potentially still be found with a search on Google's U.S. domain. For

---

191 RICHARD WHISH & DAVID BAILEY, COMPETITION LAW 11 (Oxford Univ. Press, 8th ed., 2015).

192 Eisenmann et al., *supra* note 190.

193 Zlata Rodionova, *EU Data Protection Regulation Passes in Brussels Giving Citizens Right to be Forgotten Online*, INDEPENDENT (Apr. 14, 2016), http://www.independent.co.uk/news/business/news/european-union-s-general-data-protection-regulation-privacy-facebook-data-eu-law-online-web-a6984101.html ("In [a] world where information is the most valuable currency, maintaining customer trust will be key to ensuring business success. Businesses which can't get data protection right will quickly undermine customers' trust and lose to the competition.").

194 GDPR, *supra* note 147, art. 17(2).

example, Google restricted its compliance to the Google Spain decision by removing the search results only in its European domains.[195]

Once we take into account the Internet market structure, the scope of the RTBF, and the lack of a global framework of the RTBF protection, the GDPR does not have the envisaged negative impact on the right to freedom of information.

CONCLUSION

The advancements in information technology and the amount of personal information that is increasingly uploaded and exchanged on the Internet pose serious risks of breaches of the fundamental right to protection of personal data.

In 2016, the EU legislature enacted the GDPR which recognizes and protects the RTBF as a fundamental right, enabling individuals to request and obtain from search engines providers the removal of links to personal data that are prejudicial or offensive to them. The right to be forgotten is not absolute and may be restricted for important public interest concerns, but the restriction must comply with the principle of proportionality. Accordingly, the restriction can impinge upon the individual right to data privacy protection only as much as it is necessary to achieve a legitimate goal, such as protecting the freedom of information.

The GDPR imposes on search engine providers the burden to prove not only that the proportionality principle is met but also that there are compelling legitimate grounds that justify keeping the information online, thus overriding the individual's right to keep the information private. Moreover, the GDPR imposes heavy monetary sanctions on controllers and processors that do not meet the proportionality test, which can be up to four percent of their total worldwide annual turnover of the preceding financial year.

This new regulation has been accused of imposing too great a burden on search engine providers and incentivizing them to grant every request for removal of personal data from the Internet to avoid the sanctions. If this criticism were correct, the regulation may unduly compress the right of access to

[195] Byung-Cheol Kim & Jin Yeub Kin, *The Economics of the Right to be Forgotten* 1–2 (NET Inst., Working Paper No. 15-05, 2015).

information and the freedom of expression because search engines would grant all requests to be forgotten regardless of their merits.

This Comment argued that the GDPR will not have the predicted negative impact on the right to freedom of information. First, the regulation is in line with the international law standards of the ECtHR and the ECHR that prioritize the protection of fundamental rights, particularly the right to private life, over economic interests. Second, the network effects in the Internet market will incentivize search engines to balance the right to privacy and the right to freedom of information and prevent search engine providers from removing too much information from the Internet.

On the contrary, the GDPR will not harm the right to information and will guide search engine providers to duly balance the right to be forgotten and the right to information, ensuring a more effective protection of the fundamental right to data protection.

STEFANIA ALESSI*

* Staff Member, *Emory International Law Review*; Juris Doctor, Emory University School of Law (2017); Master of Laws, The University of Chicago Law School (2014): Laurea Magistrale in Giurisprudenza, University of Palermo (2013). The author would like to thank Professor Henrikas Mickevičius for his advice and continuous support in writing this Comment. The author would also like to thank the *Emory International Law Review* Executive Board for their input throughout the editing and publication process. Finally, the author would like to thank her parents, Nicola Alessi and Luisa Tesoriere, for their encouragement.