EU Protection of the Right to Privacy and Right to Personal Data and their Connection to The *Gonzales* Case and Beyond

Remus Titiriga*

---

* Professor, Inha University, School of Law (Incheon, Republic of Korea). Email: titiriga.rem@gmail.com

Abstract

Protections of the right to privacy concerning publications have a relatively long history in Europe. The first part of the article explores comparatively and historically, the mechanisms of such protections originated in the 19th century Germany and synthesized brilliantly by Brandeis and Warren in the U.S. This part includes a brief overview of European supranational protection of the right to privacy, as framed in article 8 of the European Convention of Human Rights and, more recently, in article 7 of the EU Charter of Fundamental Rights.

The protections of the right to personal data in digital processing is a more recent occurrence in Europe. Few national constitutions or international instruments recognize such rights, and even fewer jurisdictional remedies are associated with it. There are some significant exceptions, mainly at the supranational level, such as the EU Data Protection Directive (recently replaced by the EU General Data Protection Regulation) and Article 8 of the EU Charter of Fundamental Rights. The second part of the article briefly explores these protections, their inherent logic, and the implementing mechanisms as clearly different from those characterizing the protections of the right to privacy.

The third part examines the articulation between the two protection mechanisms, as reflected by the reasoning of the European Union Court of Justice on the famous *Gonzales* case. The decision implemented a right of de-listing as "right to be forgotten on the Internet" by the search engines. We propose a new reading for the reasoning of the Court, which underlines the essential role of protections of the right to privacy in grounding and circumscribing the data protection mechanisms of the EU Data Protection Directive within the decision.

Last but not least, the article asses that the newly adopted EU General Data Protection Regulation will not affect the precedent created by the *Gonzales* and the adequate remedies it implemented.

Keywords: Right to Privacy, Personal Data Protection, Right to be Forgotten on the Internet, Right of De-listing, Data Protection Directive, General Data Protection Regulation, EU Court of Justice.

Manuscript received: December 22, 2019; review completed: April 15, 2020; Accepted: April 27, 2020

I. Introduction

De Hert and Gutwirth[1] have argued that privacy and data protection have different logic and structures. For example, privacy protection ensures that a person can choose to remain unidentified while data protection aims to provide the transparency of the processing of personal data. Therefore, the two authors contend that such a distinction is essential for drafting accurate and useful policies.

The underlining of these differences and their origin is the core purpose of this paper, such differences being relevant in understanding the real reasoning of the EU Court of Justice in *Gonzales* case.

The first part of the article starts with a brief historical examination of the European/US visions of the right to privacy in publications, and pursue by analyzing its implementing mechanism within the frame of the European Convention of Human Rights and the EU Charter of Fundamental Rights.

The second part of the paper analyzes the European/EU protections of personal data that emerged with the evolution of the digital world.

In the final part, the analysis of the legal reasoning of the EU Court of Justice (hereafter "EUCJ") in the *Gonzales* case unveils the articulation of the two protective mechanisms and its significance for the future.

II. The Emergence of a Right to Privacy Regarding Publications

A. The Two-fold Origins of the European Right to Privacy Regarding Publications

Privacy is a multidimensional concept difficult to grasp since what is considered private differs among groups, cultures, and individuals. Moreover, the sphere of privacy changes with social or technological evolution.

---

1 Paul De Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, (*Reinventing Data Protection?*, Serge Gutwirth et al. eds., Springer 2009).

The legal apprehension of a need to protect a right to privacy concerning publications[2] started in Europe (mostly in France and Germany) after the second half of the 19th century. That time some journals started to broadcast information about people in ways that endangered their public dignity.

Hence, the protection of a right to privacy in regard publications was developed initially by courts around the social values of "dignity" and "honor".[3] They included the rights to one's image, name, reputation, and, in the German context, the right to informational self-determination (the right to control the information disclosed about oneself). These were all rights to manage one's public image, guaranteeing that people see someone in the way that the person wants to be seen.

The essential developments were made in Germany, around 1880, by scholars. They built a right of personality based on protection against insult grounded on Roman sources of law[4] and in addition to the rights of creative artists.

The evolution of the law of insult was the first strand in this evolution. Jhering and several German scholars designed it based on ancient Roman law when the honor was at stake. The Romans were initially concerned only with material possessions and considered that the law could only defend pecuniary rights (or substantial rights). As concern about honor grew, those new protections gradually evolved, until the law covered all aspects of fame, protecting equally against verbal insults and other shows of disrespect. Therefore, the development of the law of honor followed the "spirit of the times",[5] in which primitive protections for merely pecuniary interests gradually matured into sophisticated protections of non-economic interests.

The slow evolution, from the material to the immaterial, lead in the modem world to what Jhering has called the law of "insulting tortious injuries".[6] The

2 The article is considering only informational privacy, the one relative to publications and media in general, and not the physical privacy. From now on, privacy and 'privacy regarding publications' will be considered as synonymous.

3 James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151, 1182 et seq. (2004), available at http://digitalcommons.law.yale.edu/fss_papers/649.

4 "Corpus Juris Civilis" and "Digestes" of Justinian, the Roman the sources of law applicable in Germany at that time, were used by the Pandekten scholars (like Jhering himself) to answer contemporary legal questions.

5 Rudolf Von Jhering & O de Meulenaere, *L'esprit du Droit Romain dans les diverses phases de son développement* (Paris : A. Marescq, Aîné, 1880).

6 See Whitman, *supra* note 3, at 1184-1185, citing Rudolf Von Jhering, *Rechtsschutz gegen injuriöse Rechtsverletzungen*, 390-396 (1885).

new protections evolved beyond protections against immaterial verbal insults to the protection of intangible goods like name, photographed image, and personal control of correspondence, as well as the access to modern conveniences such as the telegraph and the tram.

The other strand of the conceptual evolution of the German right of personality was the *Urheberrecht*[7]: creators' rights. The rights of an artistic or intellectual creator were partially covered, in German law, by copyright. Later it began to extend beyond copyright and include the author's ability to control the use of one's work by protecting one's reputation as an artist, which, according to existing continental legal terminology, was called "Droit moral de l'auteur."

In the end, the law of insult, allied with the rules of artistic creation, established a solid foundation in Germany for the protection of the right to privacy as an expression of personality rights.

B. The Contributions of Brandeis and Warren as Synthesis of the Principles for Protection of Privacy Regarding Publications

Such European developments were echoed over the Atlantic, by Samuel D. Warren and Louis Brandeis, in their famous article about "The Right to Privacy".[8] It seems that legal commentators have failed to notice that the two authors desired to transfer continental protection of privacy into US law. According to Whitman[9], Warren and Brandeis' contribution was not American innovations, but an unsuccessful continental transplant.

Warren and Brandeis applied 'mutatis mutandis' the double origin of the German right to privacy as personality right (protection against insult and the moral rights of authors). They tried to determine if the common law had precedents, principles, or legal remedies that might prevent the undesirable publication of facts about individuals. Such unwanted publications were facilitated, at that time, by new developments such as instant photography and the spread of "yellow" newspapers publishing gossip stories.

Following the German legal pattern of protection of honor in the American

---

7 *Id*.

8 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 *Harv. L. Rev. 193*, (1890).

9 *See* Whitman, *supra* note 3, at 1204.

context, Warren and Brandeis first examined the branch of tort law protecting the emotions, feelings, and ideas of persons.

They focused on the law of slander and libel (as forms of defamation) to determine if it might adequately protect the privacy of individuals. The authors concluded that this body of law could not achieve such a goal since it "deals only with damage to reputation"[10] (the protected value is the reputation of persons and their social image).

Second, shadowing the German developments, the authors examined the intellectual property rules to determine if its principles and doctrines might protect the privacy of the individuals and provide a means for preventing publication. At that time, the relevant American right of intellectual property was the copyright, which protected only the power of a creator to the profits derived from publication[11], and therefore did not recognize that there was value in preventing printing.

At this point of analysis, the authors proceeded to examine the Common law precedents regarding a person's ability to prevent publication. Warren and Brandeis observed that, although in *Prince Albert v. Strange*[12], the English court framed the decision on the protection of property, a close examination of its reasoning revealed other unspecified rights: "…where protection has been afforded against wrongful publication, the jurisdiction has been asserted, not on the ground of property, or at least not wholly on that ground, but upon the ground of an alleged breach of an implied contract or a trust or confidence".[13] In other words, the English court created a legal fiction that contracts implied a provision against publication or that a relationship of trust mandated nondisclosure.

---

10 *See* Warren & Brandeis, *supra* note 8 at 197.

11 The German (or French) moral right of authors did not have its counterpart in the US.

12 *Prince Albert v. Strange* [1849] 41 ER 1171 (Eng.) was a decision from 1849 of the High Court of Chancery of England. Both Queen Victoria and Prince Albert sketched as a hobby. Sometimes, they showed these sketches to friends or gave them away. Strange obtained some of these sketches from a person named Brown (a printer) and scheduled public viewing of these. He also published a catalog listing these sketches. Prince Albert filed suit for the return of the drawings and surrender of the catalog for destruction. A personal breach of confidence was claimed. The Court awarded Prince Albert an injunction, restraining Strange from publishing the catalog describing Prince Albert's etchings. Lord Cottenham LC (Charles Pepys, 1st Earl of Cottenham) noted that "this case by no means depends solely upon the question of property, for a breach of trust, confidence, or contract, would of itself entitle the plaintiff to an injunction." *See* at https://en.wikipedia.org/wiki/Prince_Albert_v_Strange (last visited Mar. 24, 2020).

13 *See* Warren & Brandeis, *supra* note 8, at 207.

Warren and Brandeis raised a hypothetical scenario in which the accidental recipient of a letter, who did not solicit it, opened the envelope and read the message. By merely receiving, opening, and reading the letter, the recipient does not create any contract or accept any trust.

Therefore, the two authors argued that courts had no ground to prohibit the publication of such a letter under existing theories or property rights. Instead, they argued, "the principle which protects personal writings and any other productions of the intellect or the emotions, is the right to privacy."

In the following sections, Warren and Brandeis elaborated a doctrine of the newly defined right to privacy based on "... legal analogies already developed in the law of slander and libel, and the law of literary and artistic property".[14]

For example, concerning its limits, the analogy with intellectual property implied that "the right to privacy does not prohibit any publication of matter which is of public or general interest".[15]

Based on the analogy with slander and libel the authors concluded that: "the right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel"[16] (such as proceeding in the court, parliamentary debates, etc.).

The analogy with intellectual property implied that: "the right to privacy ceases upon the publication of the facts by the individual, or with his consent".[17]

The essential differences between slander/libel as tort violating one's reputation and the unwanted publication violating the 'right to be let alone' (as of right to privacy) had as a consequence that "the truth of the matter published does not afford a defense. Obviously, this branch of the law should have no concern with the truth or falsehood of the matters published" [as is the case for libel or slander].[18]

---

14 *Id*. at 214 et seq.

15 *Id*.

16 *Id*.

17 *Id*.

18 *Id*.

Also, "the absence of "malice" [or the good faith] in the publisher does not afford a defense [as is the case for libel and slander]".[19]

Regarding the remedies, the authors established, again, by analogy with the torts of libel/slander and intellectual property rules, that a plaintiff may institute an action for damages as compensation for injury (*post-factum*) or request an injunction (*ante factum or post factum*).[20]

In conclusion, the two authors established the content of the ''right to be let alone'' as the right to privacy concerning publications, within a legal frame widely accepted today. By their nature, the rules protecting the right to privacy were *prohibitive*, meaning that their infringement was forbidden. The *matters of public interest* circumscribed the sphere of the right to privacy. The *autonomy of an individual and his free will* were part of the right to privacy since a person could modify the limits of one's private sphere (restraining them) by consenting to make facts about oneself public.

C. The Actual European Frame for Protecting Privacy Regarding Publications

The American legal practice did not embrace the conclusions of Warren and Brandeis. However, they were well received in Europe, since they brilliantly synthesized the continental vision of privacy in terms of publications and the press. The protection of privacy was later considered in Europe at national levels within omnibus privacy legislation or even as a fundamental constitutional right**.**

The fundamental right perspective was extended to the European supranational level, for example, Article 8 of the European Convention on Human Rights[21] (hereafter "ECHR") about "private life."

According to this article, "1. Everyone has the right to respect for his private and family life, his home, and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in

19 *Id*.

20 *Id*. at 219 et seq.

21 European Convention of Human Rights was adopted in 1950 following a report by the Council of Europe's Parliamentary Assembly. The Convention created also the European Court of Human Rights in Strasbourg. The practice of the Court regarding the Convention developed fully after 1970.

accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others".

This European right to privacy is not absolute and has common limiting dispositions. The first part of a rule defines the scope of the right, while the second describes its limits.

Hence, the application of the article requires a three stages proportionality test. The first step of analysis typically involves determining whether an act infringes on the scope of a right. If it does, a 'prima facie' violation of a right has occurred.

The second step consists in determining whether the infringement can be justified under the limitations clause through a three phases test (of legality, the presence of public interest or another fundamental right which might justify the interference, and the necessity test [which include another three stages tests relative to suitability, necessity-properly defined, and a proportionality test for the interfering measure]).

Only if all these successive tests were successful, the interference would not qualify as a definitive violation of the right to privacy and will be validated.

In practical terms, it seems that the concept of "private life" of the ECHR was apprehended by the European Court of Human Rights (hereafter "**ECtHR**") through the 'reasonable expectations' of privacy.[22] That means that the balancing test for deciding whether a privacy violation is necessary for a democratic society depends on the gravity of a breach. The latter relies on the way or on the amount of privacy that people should expect in a particular context.[23] It is a 'personal privacy' approach based on legitimate expectations of privacy, about moral harm and the psychological integrity of individuals,[24] grounded on a standard of the 'legitimate' (or reasonable) expectations, to be apprehended by the Court in a case-by-case development.

---

22 *See* for a fascinating discussion Cillian Gorman, *Is Society More Reasonable than You? The Reasonable Expectation of Privacy as a Criterion for Privacy Protection*, (2011) (unpublished Masters thesis, Tilburg University).

23 *Id.* at 25, citing Ronald Leenes & Bert-Jaap Koops, *'Code': Privacy's Death or Saviour?*, 19 Int'l Rev. L. Comput. & Tech., 329-340, (2005).

24 *See, f*or example, *Von Hannover vs. Germany* (No. 59320/00), 2004-VI Eur. Ct. H.R. 50 et seq.

The European Union seems to embrace a similar mechanism in its Charter of Fundamental Rights[25] (hereafter "**EUCFR**"), whose Article 7 covers the protection of the right to privacy with an almost textual reproduction of the first paragraph of Article 8 of the ECHR.

According to this article, "1. Everyone has the right to respect for his private and family life, his home, and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others". There is also a general limiting disposition for the relative rights of the EUCFR.

The first paragraph of Article 52 of the Charter clarifies that it may be acceptable for public authorities to interfere with the fundamental rights in certain circumstances: "1. Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may only be made if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. (…)". Therefore, since the right to privacy is a relative, article 52 and its limitations apply equally to the right to privacy of Article 7.[26]

III. The Emergence of an Independent Right to the Protection of Personal Data in Europe

A. The Evolution of Legal Instruments for the Protection of Personal Data

With the advancement of digital technology and databases in the 60s and 70s, it became clear that merely banning personal information exchanges, according to the restrictive rules of privacy protection, was no longer viable. New ideas

25 Drafted by the European Convention and solemnly proclaimed on 7 December 2000 by the European Parliament, the Council of Ministers and the European Commission. Its legal status was uncertain and did not have full legal effect until the entry into force of the Treaty of Lisbon on 1 December 2009.

26 However, there is no practice yet about the right to privacy on the EU level, as was the case for the ECHR.

and implementations emerged regarding the regulation of exchanges of personal data.

For example, in 1980, the Organization for Economic Cooperation and Development (OECD) issued the "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data".[27] These Guidelines, grounded on seven principles governing the protection of personal data,[28] were, however, non-binding and data privacy regulations still varied throughout Europe.

Inspired by the recommendations of the OECD, the protection of personal data was granted, as a separate individual right, in the Convention for the Protection of Individuals about Automatic Processing of Personal Data-Convention 108, adopted by the Council of Europe in 1981.

To this day, this is the only legally binding international instrument of worldwide scope.[29] However, the Convention has no direct effect since it does not creates rights and obligations that individuals might invoke before national judges. Moreover, the ECtHR has no jurisdiction over it and, therefore, there is no jurisdictional practice, either domestic or supra-national, relative to this Convention.

Realizing that divergent data protection legislation among EU member states impeded the free flow of data within the EU internal market, the European Union adopted Directive 95/46/EC (hereafter called the Data Protection Directive or Directive). It became the 'backbone' of the protection of personal data within the EU and implemented the seven principles of the OEDCD recommendations.[30]

---

27 Available at https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (last visited Mar. 24 2020).

28 These principles are relative to: notice-data subjects should know when their data are collected; purpose-data should only be used for the purpose stated and not for any other purposes; consent-data should not be disclosed without the data subject's consent; security-collected data should be kept secure from any potential abuses; disclosure-data subjects should know about whom is collecting their data; access-data subjects should be allowed to access their data and make corrections to any inaccurate data; accountability-data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

29 The treaty was open for signature by the member States and accession by non-member States. It was signed and ratified by all member States and by nine non-member States. Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (last visited Mar. 24 2020).

30 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals concerning the processing of personal data and on the free movement of such data (Council Directive 1995/46, 1995 O.J. (L 281) 31 (EC)).

The specificity of personal data protection was also proven by the adoption of the right to protect personal data as a fundamental right of the EU. The EUCFR created such a right (implementing the seven principles mentioned above) in Article 8, clearly distinct from the right to the protection of privacy of Article 7. According to article 8, "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 based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to collected data concerning him or her, and the right to have them rectified. 3. Compliance with these rules shall be subject to control by an independent authority".

B. Understanding the EU Legal Regime of the Right to Personal Data Protection

The legal logic of data protection is quite different from that of the protection of privacy. In general, *data protection regulations* are both broader and more specific than the right to privacy. They are broader because data protection also includes other fundamental rights such as freedom of expression, freedom of religion and conscience, the free flow of information, the principle of non-discrimination. Nevertheless, data protection is more specific than the right to privacy since it *only* applies when "personal data" is "processed." By default, and contrary to privacy protection, *data protection rules are not prohibitive but permissive.* They organize and control the way personal data should be processed. Personal data can be legitimately processed only when the conditions of *transparency* of processing, *the participation of the data subject*, and *accountability of the data controller* are met.

On a different level, it seems that data protection could be qualified in the EU as a fundamental right, since Article 8 of the EUCFR defines it as such, on an equal footing with the right to privacy of Article 7. However, while both fundamental rights are relative and not absolute, the similarities between the two stops here.

As relative fundamental rights of the Charter, any interference with the rights to the protection of personal data and privacy should be possible within the confines of the proportionality test defined by the first paragraph of Article 52.[31]

31 *See* the discussion in the relevant sections above.

Nevertheless, while any interference with the right to privacy (of Article 7) must satisfy a 3-stage test to be legitimate, for the right to data protection (of Article 8), such hindrance seems inconceivable. The proportionality tests in Article 8, correlate with the implementing legislation (the Directive). The Directive creates a sophisticated system of data subjects' rights regarding data processors/data controllers within a structure supervised by independent national administrative authorities or by courts. The balances between the rights of data subjects and the interests/rights of data controllers, processors, third parties are 'ínside' the scope of the rights of personal data protection. Therefore, an outer (or 'outside') balance, as for Article 7 (right to privacy), does not seems possible.

In this regard, Bart van der Sloot[32] claimed that data protection was not exactly a fundamental right. Besides other sophisticated arguments supporting his thesis, the author emphasized that the inner logic of data protection rules differs from that of fundamental rights. Data protection rules facilitate the processing activities of data and ensure that they are made fairly and adequately. The principal objective of human rights was to stop or curtail infringements on human rights. Van der Sloot also claimed that the Data Protection Directive was more akin to a market regulation than traditional human rights instruments. Such a perspective seems to rehabilitate the proprietary viewpoint that considers personal data as a commodity able to change hands.[33]

This proprietary approach became particularly popular in the US in the early 2000s.[34] During that decade, several authors, including Pamela Samuelson[35] and Paul Schwartz,[36] developed models for property-based personal data. Their contributions did not have a legal impact in the US, but they renewed the understanding of the EU data protection mechanisms.

---

32 Bart van der Sloot, *Legal Fundamentalism: Is Data Protection really a Fundamental Right?* (Ronald Leenes et al. eds., *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer International Publishing 2017).

33 *See* the fascinating considerations of Jef Ausloos, *The 'Right to be forgotten' - Worth remembering?*, 28 Comput. L. & Sec. Rev., at 3-4 (2012), available at http://ssrn.com/abstract=1970392 (last visited Mar. 24, 2020).

34 *Id.*

35 One can mention Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan. L. Rev., 1125, (2000).

36 Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117, Harv. L. Rev. 2055, (2004).

A recent example in this direction was developed by Jacob M. Victor[37] in his examination of the GDPR (but with conclusions applying 'mutatis mutandis' to the Data Protection Directive). He identified a property-based regime for data in the GDPR following the theory developed by Paul Schwartz.[38] And one can agree with Victor's conclusions (by extending them to the Data Protection Directive) that "... even though [the Directive]... is grounded in human rights rhetoric and employs no property terminology, its protections nonetheless function remarkably like the regulated property schemes. While (...) consumer protection rights are not themselves 'property rights' enforceable against third parties, they stand for a set of interests in, and burdens placed on, consumer data that can be best understood in property terms".[39]

There are clear implications for this difference of nature between the right to privacy and the right to personal data protection, in general, and in the European Union in particular. From this perspective, the inclusion in the EUCFR of Article 8 (fundamental right to data protection) after Article 7 (the fundamental right to privacy) has more a rhetorical, persuasive function. We believe that EUCFR tries to put the two rights on an equal footing even if, according to the arguments developed above, the nature, the internal logic, and the coherence of the two rights are entirely antithetical (only the right to privacy being a real fundamental right).

That might explain why the right to protection of privacy is the essential support of the right of personal data protection, in the EU Court reasoning on the *Gonzales* case, covered in the third part of the article.

37 *See* Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 Yale L.J. 513, 513-528 (2013), available at http://ssrn.com/abstract=2317903 (last visited Mar. 24, 2020).

38 *See* Schwartz, *supra* note 36.

39 *See* Victor, *supra* note 37, at 522.

IV. The Connection of the Two Rights in a Praetorian Creation of a *sui generis* 'Right to be Forgotten on the Internet' – the *Gonzales* Case

The now-famous case of the Court of Justice of the European Union (CJEU) in *Google Spain vs. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzales*,[40] was the first EU lawsuit in which the right to data protection and the right to privacy concerned the search engine service providers. Mario Costeja had suffered damage over the years because of the advertisement placed in the La Vanguardia newspaper in 1998, for a foreclosure sale related to debts he owed to the social security administration. After the journal was digitized, Google searches for the name 'Mario Costeja,' was revealing personal data and financial information that had become outdated, which affected his professional life. At first, Costeja filed a petition before the Spanish Data Protection Agency (SDPA), requesting for the newspaper to remove the information. The request was rejected. The SDPA stated that the advertisement published in the La Vanguardia newspaper was legal, and its removal would infringe upon freedom of expression. However, the SDPA sent a request to Google Spain and Google Inc., calling upon these companies to stop indexing the content above. Google filed an appeal against the agency's decision before the National High Court. This judicial authority ultimately referred for a preliminary ruling to the European Union Court of Justice. In essence, the problem for the EU Court was to recognize and circumscribe the right of Mr. *Gonzales* (or someone in his situation) to erase damaging information provided by a search engine, even if the original publication on the Internet was not erased or was impossible (legally) to erase.

The Court in its answer implemented, without calling it explicitly, a 'right to be forgotten'[41] on the Internet as a right of de-listing. The Court ordered the deletion of a web link provided by the search engine, but not the erasure of the related original article. Briefly speaking, the Court recognized that a search engine (Google in this case) "...can't forget you, but it should make you hard to find".[42]

---

40 Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzales*, 2014.

41 Such a right would imply, in principle, either removal of information on the original site, (right to erasure/deletion), either a de-listing of the original site by the search engines operator (right to de-listing/de-reference).

42 Evan Selinger & Woodrow Hartzog, *Google can't forget you, but it should make you hard to find*, (May 20, 2014), available at https://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/ (last visited Mar. 24, 2020).

Furthermore, the archetypal implications of the case were far more critical in connecting the right to privacy and the right to personal data protection. At that moment (2010-2013), the Data Protection Directive was the core of the protection of personal data within the EU. In the 1990s, when the Directive was adopted, the Internet had only become commonly used, and there were no real search engines in its actual meaning. Therefore, the historical interpretation of the Directive, focusing on the initial sense of its terms, could not solve the case. Consequently, the Court opted for an objective and progressive reading of the Directive based on textual, systematic, and teleological methods.

Nevertheless, before deconstructing the reasoning of the Court, a brief overview of the Internet as a publishing media and as personal data processing techno-environment (hence able to be apprehended by the two streams of protection rights) is necessary.

A. Identifying the Two Rights Concerning the Internet[43]

1. The Two Levels of the Internet About Personal Data Flows and the Rights to Personal Data Protection

From the perspective of data flows, there are two levels of personal data processing relevant to this case. The first level of the Internet, the World Wide Web, is a set of networked publications realized by digital means.

The second level of the Internet is the search engine providers, which produce results directing Internet users to the source web pages (the first level of the Internet). The search engine provider does not create new autonomous content. It only indicates where the existing content, made available by third parties on the Internet, can be found using hyperlinks to websites containing the search terms.

The results displayed by an Internet search engine are not based on an instant search of the whole World Wide Web. They are assembled from content previously processed by search engines. That means that the search engine has retrieved content from existing websites and copied, analyzed, and indexed that content on its own devices.

---

43 *See* for interesting hints the opinion delivered by the advocate general on 25 June 2013 in *Gonzales* Case, *supra* note 40 at 73-74.

Additionally, Internet search engines often display content alongside the link to the original website, such as text extracts, audiovisual material, or even snapshots of the source web pages. This preview information can, at least in part, be retrieved from the Internet search engine provider's devices and not from the original website. That means that the service provider holds the information displayed (in the cache memory).

2. The Right to Privacy Protection Concerning the Two Levels of the Internet as Publishing Media

The most critical element here is the publication side: the worldwide distribution of text, images, and sound facilitated by the Internet as a new mass media. As a publication, this new technical environment can infringe on individuals' privacy on a larger scale than the yellow journalism that Brandeis and Warren considered. The apprehension of such infringements requires, naturally, a personal approach to privacy, by using, for example, the legitimate expectations of privacy.

From this perspective, there are two situations. First, the Internet—the World Wide Web—is a sort of mega-text or hyper-text of publications realized by digital means. As a new sort of release, it can infringe on persons' informational privacy and require instruments and mechanisms belonging to the protection of the right to privacy (regarding publications).

The second level of the Internet, of the search engine providers, is a second-level of publishing on the Internet which, as a new mass media, can interfere even more with the privacy of persons and requires equally (and even more) the mechanisms of protection of the right to privacy (regarding publications).

The inter-correlation between the two levels and especially the higher possible interference of the second level of publishing with the right to privacy played an essential role in the Court's reasoning.

B. Deconstructing the Legal Reasoning of the Court in the *Gonzales* Case

The EU Court of Justice has no difficulty agreeing with the advocate general, Niilo Jääskinen from Finland, that the operator of a search engine was processing personal data when it linked to personal data published on the original website. Since the Directive does not impose high accountability to the processor, that qualification was less relevant.[44]

The qualification of a search engine provider as a controller, when it redirects to original web-pages containing personal data, was more consequential. It was adopted as such by the Court, contrary to its advocate general.[45]

The Court used a textual interpretation of the controller defined in Article 2(d), as the operator who "determines the purposes and means of that activity and thus of the processing of personal data that itself carries out within the framework of [search]... activity". Then, the Court took into account the purpose of Article 2(d), which "...is to ensure, through a broad definition of the concept of 'controller,' effective and complete protection of data subjects".

As final, and in our opinion, essential argument, the Court emphasized that not recognizing the quality of the controller to search engine operators would not bind them by the correlative obligations in the Directive. That would diminish the rights of data subjects, including the necessary right, *the right to privacy*.[46]

Here the core of the argument became the reasoning from effects around the right to privacy. At this point, the Court has painstakingly identified the threshold of legitimate expectations of privacy (without calling it as such) required from search engine providers, based on their increased ability to interfere with the privacy of the persons, than the original website publishers.[47]

---

44 For the publishing of personal data on web pages on the Internet (the 'web page source'), the EU Court had already given the qualification as a processing of personal data in *Bodil Lindqvist v. Åklagarkammaren i Jönköping* case (Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping,* 2003).

45 The Directive imposes an accountability system mostly to the data controller, defined as a person/entity who determines the purposes and means of personal processing data. The Directive also lists three other types of actors who can be potentially involved: data processors, third parties, and recipients of data. Relationships between a controller and a processor are governed by a contract, giving no rights to the data subject concerning the latter. Therefore, qualifying a search engine provider as the controller would ensure the broadest protection of data subjects' rights.

46 *See Gonzales* case, *supra* note 40 at 34.

47 *Id.* at 36-39.

Another group of questions concerned the responsibilities of the search engine operator as a 'controller' of personal data.

In a first sub-sub section, the problem was, in essence, whether the 'rights to erasure and blocking of data'[48] and the 'right to object'[49] of the Directive implied that the operator of a search engine must remove from the list of results, links to web pages published by third parties containing information about that person. The Court answered the question affirmatively by a systematic and literal interpretation of the Directive.[50] Briefly speaking, data subjects can demand the blocking, erasure, or destruction of data or impose a temporary or definitive ban of such processing to the search engine operator.

Moreover, the Court hinted at the balance of rights and interests[51] of search engine providers and other actors.

The Court recalled that operators of search engines might affect more significantly fundamental rights (mostly Article 7-right to privacy).[52]

Other side of the balance is the economic interest of the search engine provider. According to Court, the economic interests of search engine operators cannot justify the interference with privacy. The right to privacy must 'weigh' more, and the search engine provider should grant the removal of links. However, such removal could impact the other legitimate concerns of Internet users (their right to information-also a fundamental right of the EU Charter). According to the Court, a fair balance should be sought between these rights. The data subjects' rights override, in general, the interests-right of Internet users. However, the nature of the information in question and its sensitivity for the data subject's private life is also relevant. The public's right to information is more potent if the data

48 Article 12(b) of Directive guarantees to data subjects the right to obtain from controllers, as appropriate, "the rectification, erasure or blocking of data for which the processing does not comply with its provisions, in particular, because of the incomplete or inaccurate nature of the data."

49 Article 14(a) of Directive grants data subjects the right, "at least in the cases referred to in Article 7(e) and (f) of the directive, to object *at any time* [italics of us] on compelling *legitimate grounds* [italics of us] relating to his particular situation to the processing of data relating to him...".

50 The Court considered the *factual conditions*[italics of us], as enumerated in Article 6.1(d) relative to data quality. Since the enumeration was not exhaustive, the Court concluded that the 'right of erasure' may also arise from non-compliance with the criteria for making data processing *legitimate* [italics of us] according to the alternative conditions of Article 7(f). See *Gonzales* case, *supra* note 40, at 62-78.

51 *See Gonzales* case, *supra* note 40, at 81.

52 The systematic mentioning of Article 8 (the right to personal data protection) of EUCFR in these various contexts by the Court had only an ideological-rhetorical character since, as seen supra, the right to protect personal data is not a fundamental right.

subject plays a particular role in public life (as a public figure).[53]

The next sub-question asked whether the 'rights to erasure and blocking of data' and the 'right to object' against the search engine operator exist even if the name or information is not erased beforehand or simultaneously from the original web pages. The Court's answer was equally affirmative, with arguments revolving once again around the protection of the right to privacy.[54]

The essential part of the Court's argument was reasoning from effects concerning the effective remedies for privacy infringements in the two situations. The two must decouple since making the remedy against a search engine provider (the de-listing) dependent on a successful initial remedy against the original publisher (the deleting) would make the former ineffective.

Furthermore, other arguments of the Court support the different treatments of two situations.

At first, there is a possible difference between legitimate grounds for data processing, according to the Directive[55] which creates different outcomes. If the grounds for legitimate processing were similar, the balance with the right to privacy is not necessarily identical since the data processing carried out by the search engine affects data subjects' rights to privacy more significantly than the original publications on the Internet.

C. The Role Played by the Right to Privacy in *Gonzales* Case

The *Gonzales* case was under the regime of the Data Protection Directive. Besides textual and systematic arguments, the search engine providers were recognized by the Court as controllers of personal data, mainly because they can infringe the right to privacy on a massive scale.

Here the data protection mechanisms of the Directive were grounded by the Court, within a finalist reasoning, on the protection of the right to privacy, with an implicit use of the legitimate expectations of privacy,[56] while a higher

53 Once again, the unnamed legitimate expectations of privacy have an essential role in the argument.

54 *See Gonzales* case, *supra* note 40, at 80-88.

55 For example, the original publishers on the internet can follow a non-pecuniary interest-the right to information of journalism. At the same time, a search engine provider always has an economic interest.

56 The Court never use the concept openly as such.

threshold was required, for obvious reasons, from the search engine providers.

Once the search engine providers were considered controllers of personal data, they have the obligations of controllers with the appropriate remedies for the data subjects. These remedies were based on 'reasons to erasure and blocking of data' of Article 12(b) and 'right to object' of Article 14(a) of Directive.

Subsequently, the Court clarified the legal situation of the search engine providers regarding the original web pages publishers with arguments revolving once again around the protection of the right to privacy. The Court re-acknowledged that the data processing carried out in the context of a search engine is added to that of publishers of websites and affects data subjects' fundamental rights to privacy more significantly than the original publisher. Therefore the Court impose higher obligations for the search engine providers, uncorrelated with eventual obligations for the web publishers. The Court also acknowledged that remedies against a search engine provider would be much more effective.

One can conclude that the data protection mechanisms of the Directive were quasi-subordinated by the Court to the protection of the right to privacy, with an implicit use of legitimate expectations of privacy. This quasi-subordination regarding search engine providers was inevitable since the *Gonzales* case concerned the publishing activity (at the first or second level) on the Internet.

There is a particular relation between the two protective mechanisms and rights. For example, if a processor or controller of personal data is infringing data protection rules, it might not infringe the right to privacy if personal data do not become public (are not 'published' and seen by the public, the 'eyes of the people'). In such a case, the right to privacy cannot play any role. However, when personal data become public, the protection of privacy becomes essential and prevails over the mechanisms of data protection. That was the specific situation in the *Gonzales* case. Absent the publishing nature of the interaction, the right to privacy would not manifest itself, and the right to be forgotten as a right to de-listing on the Internet would cease to exist.

D. Looking Beyond *Gonzales* Case

The Data Protection Directive was replaced, since 25th May 2018 by the GDPR.[57] The new Regulation made several changes to the architecture of personal data protection created by the Directive.

It seems that controllers will have more obligations, and, accordingly, data subjects will be better protected. The 'right to object to processing' in Article 14(a) of the Directive become Article 21 of the GDPR. The 'right to erasure' (removal of information) in the Article 12(b) of the Directive, was replaced by

Article 17 of the GDPR (which introduces for data subjects an explicit 'right to the erasure' of personal data).

The 'right to be forgotten on the Internet' as de-listing, formulated by the Court in *Gonzales* case, will rest unchanged under the GDPR. The right to privacy of data subjects and the retrieved balance with other rights and interests will still exist, even within a changed enumeration or new articles. Hence, the responsibility of search engine providers for the infringement of privacy by publishing personal data of data subjects on the Internet, and the remedy of de-listing such results, will continue unabated under the new Regulation.

Furthermore, under the new Regulation, the 'right to be forgotten' as a right of de-listing specific results on the Internet by search engine providers,[58] intimately linked to the right to protection of privacy, will be much more useful than the new 'right to the erasure of personal data' in general.

V. Conclusion

The first part and the second part of the article differentiated, within a European and historical context, the protections of the right to privacy (concerning publications) and the right to protection of personal data (regarding digital processing) with their inherent logic and the implementing mechanisms.

---

57 General Data Protection Regulation ("GDPR"), Council Regulation EU 2016/679, 2016 O.J. (L 119) 1 (EC).

58 This remedy will be much more effective and protective of the data subjects than the 'right to be forgotten' as 'right to erasure' explicitly introduced by GDPR in article 17.

The third part of the article examined the articulation between these protections, as reflected in the reasoning of the European Union Court of Justice on the *Gonzales* case. That decision created a "right to be forgotten on the Internet," where the right to privacy supported, through a finalist and progressive argumentation, the right to protect personal data. This connection was made possible by understanding the Internet as a new publishing instrument, besides the apparent use of computing instruments. Moreover, the decision created a 'right to be de-listed,' as a more robust and more efficient remedy than the 'right to erasure' in general, which was introduced more recently by the GDPR.

We believe that the duality of the universal transparency and the ubiquitous computing, which characterize our information society, will connect the right to privacy and the right to personal data processing in the future practice of the European Union Court of Justice.

Bibliography

Books

Rudolf Von Jhering & O de Meulenaere, L'esprit du Droit Romain dans les diverses phases de son développement (Paris: A. Marescq, Aîné, 1880).

Rudolf Von Jhering, *Rechtsschutz gegen injuriöse Rechtsverletzungen,* Yearbooks for the dogmatics of today's Roman and German private law (1885).

Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth & Paul De Hert, Data Protection and Privacy: (In)visibilities and Infrastructures, (Springer International Publishing 2017).

Articles

Paul De Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action* (Reinventing Data Protection?, Serge Gutwirth et al. eds., Springer 2009).

James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151, (2004).

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, (1890).

Cillian Gorman, *Is Society More Reasonable than You? The Reasonable Expectation of Privacy as a Criterion for Privacy Protection*, (2011) (unpublished Masters thesis, Tilburg University).

Bart van der Sloot, *Legal Fundamentalism: Is Data Protection really a Fundamental Right?* (Ronald Leenes et al. eds., Data Protection and Privacy: (In)visibilities and Infrastructures, Springer International Publishing 2017).

Ronald Leenes & Bert-Jaap Koops, '*Code': Privacy's Death or Saviour?*, 19 Int'l Rev. L. Comput. & Tech., 329-340, (2005).

Jef Ausloos, *The 'Right to be forgotten' - Worth remembering?*, 28 Comput. L. & Sec. Rev., 3-4 (2012).

Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan. L. Rev., 1125, (2000).

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117, Harv. L. Rev. 2055, (2004).

Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 Yale L.J. 513, 513-528 (2013).

Cases

Prince Albert v. Strange [1849] 41 ER 1171 (Eng.).

Von Hannover vs. Germany (No. 59320/00), 2004-VI Eur. Ct. H.R. 50.

Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzales*, 2014.

Case C-101/01, *Bodil Lindqvist v. Åklagarkammaren i Jönköping,* 2003.

European Union Legislative Materials

Council Directive 1995/46, 1995 O.J. (L 281) 31 (EC).

Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EC).

Internet Sources

Organization for Economic Cooperation and Development (OECD), *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data*, (1980), available at https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.

Convention for the Protection of Individuals about Automatic Processing of Personal Data-Convention 108, available at https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.

Evan Selinger & Woodrow Hartzog, *Google can't forget you, but it should make you hard*

to find, (May 20, 2014), available at https://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/.