# RIGHT TO BE FORGOTTEN: MUCH ADO ABOUT NOTHING

*Giancarlo F. Frosio*[*]

**ABSTRACT**

*In the information society, the role of private sector entities in gathering information for and about users has long been a most critical issue. Therefore, intermediaries have become a main focus of privacy regulations, especially in jurisdictions with a strong tradition of privacy protection such as Europe. In a landmark case, the European Court of Justice (ECJ) ruled that an Internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties. The recognition by the European Union of a so-called "right to be forgotten" (RTBF) has ignited disgruntled reactions from civil society and legal scholars, especially in the United States. Meanwhile, proposals for the adoption of a similar right have appeared in several jurisdictions, including Brazil, Japan, Korea, and Russia. Supposedly, the right to be forgotten would endanger freedom of expression (FoE) and access to information. Apparently, factoids—defined by the Oxford Dictionary as "an item of unreliable information that is reported and repeated so often that it becomes accepted as fact"—dominated the recent debate surrounding the right to be forgotten. This article will discuss and debunk these factoids, review data protection legislation in Europe, and explore the legal and policy implications of the newly emerging right to be forgotten. Finally, the idea that extra-territorial application of the RTBF might unleash a kraken that can break down the Internet will be contextualized within the present political scenario. The extra-territorial application of the RTBF follows in the footsteps of a global move towards data protectionism against the de facto market dominance of US Internet conglomerates. Global blocking governed by a nationality principle—as suggested by the French Privacy Authority (CNiL) and other EU institutions—would put at rest these protectionist concerns.*

## 1. Introduction

In a landmark case, *Google Spain v. Costeja*, the European Court of Justice ruled that an Internet search engine operator is responsible for the processing of personal data that it carries out which appear on web pages published by third parties.[1] Thus, under certain

[*]Senior Researcher and Lecturer, Center for International Intellectual Property Studies (CEIPI), Universitè de Strasbourg; Non-Resident Fellow, Stanford Law School, Center for Internet and Society. S.J.D., Duke University School of Law, Durham, North Carolina; LL.M., Duke University School of Law, Durham, North Carolina; LL.M., Strathclyde University, Glasgow, UK; J.D., Università Cattolica del Sacro Cuore, Milan, Italy. The author can be reached at gcfrosio@ceipi.

[1] *See* Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12 (ECJ, May 13, 2014), *available at* https://cyberlaw.stanford.edu/page/wilmap-

circumstances, search engines can be asked to remove links to webpages containing personal data. The plaintiff Mr. Costeja asked to have records regarding a past conviction—a 1998 notice of real estate auction following attachment procedures for the recovery of Social Security debts—delisted from Google search entries resulting from searches based on Costeja's name. As the ECJ originally states, the rights of the data subject "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name."[2] Following the case, any search engine operating in Europe must remove from its search results the links to personal information if this is ''inaccurate . . . inadequate, irrelevant or excessive in relation to the purposes of the processing.''[3] This right—finally recognized by the ECJ—strongly resembles the French right of oblivion, which allows an individual to object to the publication of information regarding a conviction after the sentence has been served and rehabilitation has occurred.[4] However, the roots of the right to be forgotten extend far beyond the right to oblivion to reach more critical checks and balances in the European human rights tradition.

Shortly after the *Google Spain* ruling, the European Parliament adopted the new General Data Protection Regulation (GDPR), which includes a "Right to Be Forgotten" provision—also known as right to erasure—with specified steps for data controllers to erase information upon request.[5] In addition, according to Article 18 of the GDPR—also known as the "restriction right"—the data subject "shall have the right to obtain from the controller restriction of the processing" of personal data.[6] When processing is restricted, data controllers are permitted to store the personal data, but not further process it. The controller must render the data inaccessible, rather than deleting it as in the case of the right to be forgotten. The data subject is entitled to the right to erasure in miscellaneous specific circumstances, including when "the personal data are no longer necessary in

---

european-union (clarifying that (1) Search engines qualify as data controllers under Directive 95/46/EC to a search engine insofar as (a) the processing of personal data is carried out in the context of the activities of a subsidiary on the territory of a Member State, (b) set up to promote and sell advertising space on its search engine in this Member State with the aim of making that service profitable. In this case, the processing of data by search engines, "must be distinguished from, and is additional to that carried out by publishers of third-party websites"); Christopher Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges*, in PROTECTING PRIVACY IN PRIVATE INTERNATIONAL AND PROCEDURAL LAW AND BY DATA PROTECTION 19-55 (Burkhard Hess and Cristina M. Mariottini (eds.), Ashgate 2015), *available at* http://ssrn.com/abstract=2496060; Brendan van Alsenoy, Aleksandra Kuczerawy, Jef Ausloos, Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril? (ICRI Research Paper 15/2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494.

[2] Google Spain, *supra* note 1, at § 97.

[3] *Id*, at § 92.

[4] *See* Mariarosaria Taddeo and Luciano Floridi, *The Debate on the Moral Responsibility of Online Service Providers*, Sci. Eng. Ethics 1, 18 (published online November 27, 2015), *available at* http://link.springer.com/article/10.1007%2Fs11948-015-9734-1.

[5] *See* Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1 [hereinafter GDPR], at Art. 17.

[6] *Id*., at Art. 18.

relation to the purposes for which they were collected or otherwise processed."[7] In contrast, the "right to restriction of processing" does more narrowly apply, *inter alia*, to cases where "the accuracy of the data is contested by the data subject."[8] The restriction of processing should happen immediately upon the data subject's request and last "for a period enabling the controller to verify the accuracy of the data."[9] These norms replace—and better qualify—the provisions on erasure and blocking of data in the Data Protection Directive.[10] However, the GDPR's practical implementation will take some time before being tested as the new regulation will take effect beginning on May 25, 2018.

Meanwhile, proposals for the adoption of a similar right—as well as judicial enforcement or rejection of the same—have appeared in several jurisdictions, including Argentina,[11] Brazil,[12] Chile,[13] Colombia,[14] Mexico,[15] Nicaragua,[16] Japan,[17] Korea,[18] and

---

[7] *Id*., at Art. 17(a)

[8] *Id*., at Art. 18(a).

[9] *Id*.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, Art. 12 [hereinafter DP Directive], *available at* http://cyberlaw.stanford.edu/page/wilmap-european-union.

[11] *See* Rodriguez M. Belen c/Google y Otro s/ daños y perjuicios, R.522.XLIX (Corte Suprema [Supreme Court], October 29, 2014) (Argentina), *available at* http://cyberlaw.stanford.edu/page/wilmap-argentina (acquitting Google and other search engines from liability for linking in search results to third-party content that violates fundamental rights); *see also* Edward L. Carter, *Argentina's Right to Be Forgotten*, 27 EMORY INT'L L. REV. 23 (2013).

[12] *See* Bill No. 215/2015 (Brazil), *available at* http://www2.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=9242F3D0D2153233D3474BAA94BA53FA.proposicoesWeb1?codteor=1395933&filename=Parecer-CCJC-06-10-2015; Bill No. 7781/2014 (Brazil), *available at* http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?_codteor=1270760&filename=PL+7881/2014; *see also* Draft Bill 215/2015, Infanticide to the Newly-born Digital Rights in Brazil, Digital Rights Newsletter N. 27, October 27, 2015), *available at* http://www.digitalrightslac.net/en/proyecto-de-ley-2152015-infanticidio-contra-los-recien-nacidos-derechos-digitales-en-brasil; Brazilian Congressman Introduces Right to Be Forgotten Bill, Information Security Blog, October 23, 2014, https://www.huntonprivacyblog.com/2014/10/articles/brazilian-congressman-introduces-right-forgotten-bill;.

[13] *See* The Regulatory Framework for Data Protection in Chile and Future Challenges, Global Data Hub (May 2015), https://united-kingdom.taylorwessing.com/globaldatahub/article_dp_cyber_chile.html (mentioning that a bill was prepared but a final draft not yet presented to the Congress).

[14] *See* Gloria v. Casa Editorial El Tiempo, T-277/15 (Colombian Constitutional Court, May 12, 2013), *available at* https://cyberlaw.stanford.edu/page/wilmap-colombia (stating that when there is a favorable outcome for an individual in a proceeding—in this case Gloria was acquitted from charges of human trafficking—there is an obligation to update the information and make the outdated information unavailable through searches; however, this obligation would apply only to media outlets—*el Tiempo* in this instance—which should ensure, using available Internet tools, that search engines would be unable to find the article, while ordering Google to block an article linking another individual to human trafficking would amount to a form of prior censorship); Martínez v. Google, T-040/13 (Colombian Constitutional Court, January 28, 2013), *available at* http://cyberlaw.stanford.edu/page/wilmap-colombia (noting that Google was to be acquitted because it ""provides a service for searching for information that is on the entire Internet. The company does not write or publish such information, but is simply a search engine; it may not be held liable for the veracity or impartiality of any article, story, or column appearing in its search results.")

[15] *See* Carlos Sánchez de la Peña v. Google México, S. de R.L., PPD.0094/14 (National Institute for the Access to Information, January 2015), *available at* http://http/inicio.ifai.org.mx/pdf/resoluciones/2014/PPD94.pdf (ordering Google Mexico to remove embarrassing—but true—search results about a prominent

Hong Kong.[19] Most notably, in July 2015 Russia was the first country signing a bill enforcing the right to be forgotten into law.[20]

The recognition by the European Union of a so-called "right to be forgotten" has ignited disgruntled reactions from US legal scholars and elsewhere.[21] Skeptics argue that the right to be forgotten would endanger freedom of expression and access to information

---

businessman. The INAI ruled in favor of a transportation magnate, Carlos Sánchez de la Peña, who wanted three links removed from Google search results. The links contained negative comments about the business dealings of Mr. Sánchez's family—including a government bailout of bad loans. The INAI heard the case after Google Mexico rejected a petition from Mr. Sánchez to have the links removed. The INAI commissioners considered that Mr. Sánchez met the privacy-law requirements that allow for the removal of information when its "persistence causes injury" even if the information was lawfully published. Mexico's data privacy law contains exceptions to Internet privacy rules if the information is in the public interest. The INAI, however, did not apply the exception, arguing that Google didn't claim those exceptions when making its case. The INAI ordered the removal only from google.com.mx. Mexico's data privacy law only requires the removal of links from local search engines. The INAI ruling was finally appealed before the ordinary courts.)

[16] *See* Ley N. 787/2012 (Nicaragua), Art. 10, *available at* http://www.oas.org/es/sla/ddi/docs/N3%20Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf.

[17] *See* XXX v. Google (Tokyo High Court, July 12, 2016) (rescinding a judgment from the District Court of Saitama that recognized the "right to be forgotten" in a case filed by a man who demanded Google Inc. eliminate five-year-old articles on his crime record from its search results).

[18] *See* Korea Communications Commission (KCC), Guidelines on the Right to Request Access Restrictions on Personal Internet Postings (April 29, 2016) (providing—as early as June 2016—to individuals the right to request web operators or service providers to restrict the public from accessing postings that were personally uploaded in the past ("personal internet postings"), and to ultimately remove this online information.)

[19] *See* David Webb v. Privacy Commissioner for Personal Data, No. 54/2014 (Hong Kong Administrative Appeal Board, October 27, 2015), *available at* https://www.pcpd.org.hk/english/files/casenotes/AAB_54_2014.pdf (requiring Mr. Webb remove from webb-site.com the names of parties set out in court judgments of matrimonial proceedings published on the Hong Kong judiciary's website over a decade earlier); *see also* Eastweek Publisher Limited & Another v Privacy Commissioner for Personal Data [2000] 2 HKLRD 83, available at http://www.hklii.hk/eng/hk/cases/hkca/2000/442.html (according to which "it is [. . .] of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify"; therefore, an argument was made that under Hong Kong law search engines could data users—which equal EU data controllers—as they do not collect data).

[20] *See* Federal Law No. 264-FZ (aka Right to be Forgotten Law) (July 13, 2015) (imposing an obligation—with some exceptions—on search engines that disseminate advertisements targeted at consumers located in Russia to remove search results listing information on individuals where such information is unlawfully disseminated, untrustworthy, outdated, or irrelevant).

[21] *See* Jeffry Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2015),; Bolton Robert Lee, *The Right to Be Forgotten, Forced Amnesia in a Technological Age*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 133 (2015); Jonathan Zittrain, Don't Force Google to Forget, NEW YORK TIMES, May 14, 2014, http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0; Annemarie Bridy, Google Spain and the Right to Be Forgotten, FREEDOM TO THINKER BLOG, May 14, 2014, https://freedom-to-tinker.com/blog/abridy/google-spain-and-the-right-to-be-forgotten; Henry Farrell and Abraham Newman, Forget Me Not, FOREIGN AFFAIRS, May 15, 2014 http://www.foreignaffairs.com/articles/141435/henry-farrell-and-abraham-newman/forget-me-not; Miquel Peguera, The Shaky Ground of the Right to Be Delisted, 15 VAND. J. ENT. TECH L. 507 (2015); Stefan Kulk and Frederik J. Zuiderveen Borgesius, *Google Spain v. González: Did the Court Forget About Freedom of Expression?*, EUROPEAN JOURNAL OF RISK REGULATION (2014), *available at* http://ssrn.com/abstract=2491486.

to the extent that—according to the most concerned views—it might corrupt history.[22] The debate has struggled with the balance between privacy and freedom of expression, which has become a conundrum increasingly hard to disentangle in the online environment.[23] According to a Communication on open journalism from the Organization for Security and Cooperation in Europe, "the legitimate need to protect privacy and other human rights should not undermine the principal role of freedom of the media and the right to seek, receive and impart information of public interest as a basic condition for democracy and political participation."[24] In addition, miscellaneous—and opposing—international approaches in balancing the competing rights at stake have steadily polarized the debate. As Professor Floridi and Taddeo noted,

> [s]triking the correct balance between the two is not a simple matter. Things change, for example, depending on which side of the Atlantic one is. According to the European approach, privacy trumps freedom of speech; whereas the American view is that freedom of speech is preeminent with respect to privacy. Hence, defining the responsibilities of OSPs [online service providers] with respect to the right to be forgotten turns out to be quite problematic, as it involves the balancing of different fundamental rights as well as considering the debate on the national versus international governance of the Internet.[25]

As expected in a matter that has grown more and more polarized, factoids dominated the recent debate surrounding the right to be forgotten. The Oxford Dictionary defines factoid as "an item of unreliable information that is reported and repeated so often that it becomes accepted as fact."[26] According to the World Association of Newspapers and News Publishers, two years after the decision "some of the most belligerent opinions on the ruling appear to be largely based on misinformation."[27] One common factoid is related to the nature and genesis of the right to be forgotten and whether it is a wholly

---

[22] *See* Geoffrey King, EU"Right to be Forgotten" Ruling Will Corrupt History, Committee to Protect Journalists (CPJ) Blog, June 4, 2014, https://cpj.org/blog/2014/06/eu-right-to-be-forgotten-ruling-will-corrupt-histo.php.

[23] *Cf*., *e.g.*, Google Brazil v Dafra, Special Appeal No. 1306157/SP (Superior Court of Justice, Fourth Panel, 24 March 2014), available at https://cyberlaw.stanford.edu/page/wilmap-brazil (stressing the importance of imposing liability on intermediaries by noting that "violations of privacy of individuals and companies, summary trials and public lynching of innocents are routinely reported, all practiced in the worldwide web with substantially increased damage because of the widespread nature of this medium of expression."); Delfi AS v Estonia, No. 64569/09 (ECHR 2015), § 110 (upholding the protection of the right to privacy against freedom of expression, after noting that, in the internet, "[d]defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online.")

[24] Organization for Security and Cooperation in Europe (OCSE) Representative on Freedom of the Media, Dunja Mijatović, 3rd Communiqué on Open Journalism, Vienna, January 29, 2016, at 2 http://www.osce.org/fom/219391?download=true.

[25] Taddeo and Floridi, *supra* note 4, 18-19.

[26] Oxford Dictionary Online, Factoid, https://en.oxforddictionaries.com/definition/factoid.

[27] *Cf*. Elena Perotti, WAN-IFRA Report on Right to be Forgotten: the Myths, the Facts and the Future, WAN-IFRA Blog, April 15, 2016, http://blog.wan-ifra.org/2016/04/15/wan-ifra-report-on-right-to-be-forgotten-the-myths-the-facts-and-the-future (noting also that that newspapers have less to fear from the Right to be Forgotten than what conventional wisdom suggests); *see also* ELENA PEROTTI, RIGHT TO BE FORGOTTEN: THE EUROPEAN RULING AND ITS EXTRA-EU IMPLEMENTATION (WAN-INFRA Public Affairs Media Policy, March 31, 2016), *available at* http://www.wan-ifra.org/sites/default/files/field_article_file/WAN-IFRA_Right_Forgotten_0.pdf.

new right. Other factoids pertain to the extent of the right, which would allegedly silence freedom of expression. Also, factoids encompass the practical implementation of the right and chilling effects on technological innovation. In the following sections, I will discuss and debunk some of these factoids.

## 2. ~~RTBF~~ The Right to Be Forgotten, Human Dignity, and Informational Self-determination

Much confusion surrounds the nature and genesis of the right to be forgotten including questions including: Should we have a right to be forgotten online? Is it a wholly new creation of the European Court of Justice? In Europe, a right to be forgotten has long been recognized—at least as long as European courts have acknowledged a right to informational self-determination. The term informational self-determination was first used in the context of a German constitutional ruling relating to personal information collected during the 1983 census.[28] The German term is *informationelle Selbstbestimmung*. On that occasion the German Federal Constitutional Court ruled that:

> [...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the German constitution. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest.[29]

The right of informational self-determination is a critical achievement in empowerment of users' rights. It was embedded in Article 12(b) of the Data Protection Directive by the rule that allows a data subject to request "rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[30] The right to be forgotten just ported the right of informational self-determination to the digital domain by making search engines data controllers, and thus subject to the Directive's provisions. The right of informational self-determination empowers individuals against data processing entities—such as advertisers, insurers, supermarkets, big pharma, and data brokers—by guaranteeing the "authority of the individual in principle to decide for himself whether or not his personal data should be divulged or processed."[31] The German Court vested this right with constitutional value. The UK legal tradition has also endorsed the essence of this right—although framing it within a property, rather than a human right

---

[28] BVerfGE 65, 1 vom 15.12.1983 (Volkszahlungs-Urteil) translated in English by Eibe Riedel *in* 5 HUMAN RIGHTS L. J. 94, 94-116 (1984); *see also* Eibe Riedel, *New Bearings in German Data Protection – Census Act 1983 Partially Unconstitutional*, 5 HUMAN RIGHTS L. J. 67 (1984); Gerrit Hornung and Christoph Schnabel, Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination, 25(1) COMPUTER LAW & SECURITY REVIEW 84 (2009); Antoinette Rouvroy and Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, *in* REINVENTING DATA PROTECTION? 45-76 (Serge Gutwirth et al eds., Springer 2009)

[29] BVerfGE 65, 1, *supra* note 28.

[30] DP Directive, *supra* note 10, at Art. 12.

[31] Riedel, *supra* note 28, at 69.

perspective—by noting that "if information is my private property, it is for me to decide how much of it should be published."[32] In recent times, this fundamental right has been qualified as a right to human dignity that serves as a foundation for the right to privacy.[33] The recently enacted General Data Protection Regulation makes specific reference to the fact that rules [for processing in the context of employment] "shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights."[34]

At early stages of the information society, Europe decided to prevent the emergence of business models based on the exploitation of the "privacy myopia."[35] According to Professor Fromkin, privacy myopia might lead to the death of privacy as individuals have been surrendering their privacy bit by bit by giving away their data too often and too cheaply.[36] In fact, Fromkin thought that all was not lost, but of course that was long time ago. Then came Facebook—and the NSA. To put it bluntly, unlike Europe, other jurisdictions endorsed different policy strategies that lead to the unstoppable growth of businesses that have been thriving on the privacy myopia.

## 3. Balancing the Right to Be Forgotten and Freedom of Expression in Europe

There is a misplaced assumption that "Europe is exporting censorship all over the world."[37] Actually, the right to be forgotten debate is about 'data protection v. economic interests,' rather than 'data protection v. freedom of expression'.[38] Misperceptions regarding the extent of the RTBF—and in particular whether the ECJ ruling and later developments did not take into adequate consideration freedom of expression—should be put at rest once for all.

---

[32] McKennit v. Ash [2006] EWCA Civ. 1714, § 55 (Lord Justice Buxton).

[33] See Luciano Floridi, On Human Dignity as a Foundation for the Right to Privacy, Philosophy and Technology 1 (2016); *see also* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW (Oxford University Press 2015).

[34] *See* GDPR, supra note 5, at Art. 88; s*ee also* European Parliament, Press Release, New EU rules on data protection put the citizen back in the driving seat, December 17, 2015, http://goo.gl/vGdMCA; European Commission, Reform of EU Data Protection Rues, http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

[35] insert citation.

[36] *See* Michael Fromkin, *The Death of Privacy?*, 52 STANFORD LAW REVIEW 1461, 1502-1503 (2000)

[37] Edison Lanza, Freedom of Expression Rapporteur of the Inter-American Commission on Human Rights, WS 142 Cases on the Right to be Forgotten, What Have we Learned?, Internet Governance Forum 2015.

[38] See Jef Ausloos and Aleksandra Kuczerawy, *From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain Ruling*, 14 COLO. TECH. L.J. (2016); *see also* Meg Leta Ambrose and Jef Ausloos, *The Right to Be Forgotten Across the Pond*, 3 J. OF INF. POL'Y 1, 1-23 (2013)

### *3.1. The Construction of the Necessary Balancing between Privacy and Freedom of Expression by European Institutions*

There is an existing belief that the *Google Spain* decision "forgot" about freedom of expression.[39] This is not the case, as made clear both by the original ECJ ruling and its subsequent construction and implementation. The ECJ stated that the person's right to privacy generally overrides "as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name."[40] This is not surprising as privacy itself is censorship and stands in contradiction with FoE. Privacy is about *not* circulating information regarding a specific person. Privacy therefore defines the boundaries of FoE, not *vice versa*. However, the ECJ also noted that this general rule should not apply if there is a preponderant interest of the general public in having access to the information "for particular reasons, such as the role played by the data subject in public life."[41]

Furthermore, the ECJ referred to an exception "for journalistic purposes,"[42] which would exempt news publishers from the right to be forgotten—originally Article 12(b) of the DP Directive.[43] That exemption would not apply to the processing carried out by a search engine but it could very well happen. The ECJ notes that the right to be forgotten cannot be exercised against the publisher of the web page if the processing was carried out "solely for journalistic purposes."[44]

In addition, the ECJ explicitly considered freedom of expression in its ruling as a pre-requisite to the implementation of the right to be forgotten, according to traditional rules governing the necessary balancing between privacy and FoE. In discussing the legal contest—and therefore the necessary balancing of rights that national courts should apply—the ECJ mentions that Article 9 of Directive 95/46, titled 'Processing of personal data and freedom of expression', provides:

> Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[45]

This reference should have sufficed in light of the scope of the ECJ jurisdiction in this case. The *Costeja* referral was asking the court whether search engines are data controllers, rather than whether or how freedom of expression and privacy have to be balanced in this specific context. Absent an "absolute first amendment"—privacy and freedom of expression needs to be equally balanced in Europe according to Articles 8 and

---

[39] *See, e.g.*, Kulk and Borgesius, *supra* note 21.

[40] Google Spain, *supra* note 1, at § 81.

[41] *Id.*

[42] *See* DP Directive, *supra* note 10, at Art. 9.

[43] *Id.*, at §85

[44] *Id.*

[45] *Id.*, at § 9.

10 of the European Convention of Human Rights.[46] The actual balancing of rights that cases like *Costeja* may require is left to national courts and privacy authorities.

This reference to the necessary balancing between privacy and freedom of expression was soon picked up by other European authorities and national courts to be implemented into full-flagged safeguards for freedom of expression against the right to be forgotten. On November 26, 2014, the European data protection authorities (DPAs) assembled in the Article 29 Working Party (WP29) adopted guidelines on the implementation of the ECJ judgment.[47] These guidelines contain the common interpretation of the ECJ's ruling as well as common criteria to be used by the national DPAs when addressing complaints. According to WP29, a balance must be made between the nature and sensitivity of the data and the interest of the public to have access to that information.[48] However, if the data subject plays a role in public life, the interest of the public will be significantly greater.[49] Therefore, the guidelines concluded, the impact of de-listing on individual rights to freedom of expression and access to information will be very limited. When DPAs assess the relevant circumstances, de-listing will not be appropriate, if the interest of the public overrides the rights of the data subject.[50] The guidelines also contain thirteen main criteria which the national DPAs will apply to handle the complaints following refusals of de-listing by search engines.[51] Freedom of expression safeguards dominate these criteria, which will be applied on a case by case basis and have to be read in the light of the "the interest of the general public in having access to [the] information."[52]

Also, balancing of the RTBF with competing rights comes from the recently enacted General Data Protection Regulation. Although, the GDPR will be applicable only from May 25, 2018—and it is hard to foresee how the GDPR's provisions will be applied in practice—multiple safeguards for FoE have been embedded in the text. In particular, the provision on the right to be forgotten, Article 17, remarkably states that the controller's obligation shall not apply to the extent that data processing is necessary "for exercising

---

[46] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 213 U.N.T.S. 221, ETS 5, 4 November 1950, at Art. 8 and 10.

[47] *See* Article 29 Data Protection Working Party, Guidelines on the Implementation of the CJEU Judgment on Google Spain v. Costeja, 14/EN WP 225 (November 26, 2014) (hereinafter WP29 Guidelines), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf; *see also* Giancarlo Frosio, *EU Data Protection Authority Adopts Guidelines on the Implementation of the Right to be Forgotten*, CIS Blog, November 28, 2014, https://cyberlaw.stanford.edu/blog/2014/11/eu-data-protection-authority-adopts-guidelines-implementation-right-be-forgotten (summarizing the WP29 Guidelines).

[48] WP29 Guidelines, *supra* note 47 at 2.

[49] *Id*.

[50] *Id*.

[51] Id., at 13-19 (providing a number of specific suggestions for the DPAs to interpret and properly balance each criterion)

[52] *Id*., at 11; *see also* Jef Ausloos and Aleksandra Kuczerawy, *From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain*, 14 COLO. TECH. L. J. 219 (2016) (studying what can be learned from the ongoing discussions in the Notice-and-Takedown context, to ensure proper procedural safeguards for implementing the 'right to be delisted').

the right of freedom of expression and information."[53] Again, the same provision shall not apply if the processing is necessary "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" in so far the right to be forgotten "is likely to render impossible or seriously impair the achievement of the objectives of that processing."[54] Also, the "media exception" of the GDPR appears substantially broader than its equivalent in the earlier Data Protection Directive. The exception is no longer limited to data processing "carried out solely for journalistic purposes or the purpose of artistic or literary expression."[55] Rather, the exception aims more generally to reconcile data protection rights with "the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression."[56] Finally, in the case of the "right to restriction of processing"—which was newly qualified by the GDPR as mentioned earlier—the controller must restrict the processing—and thus render the data inaccessible—immediately upon the claim and "for a period enabling the controller to verify the accuracy of the personal data."[57] Indeed, the legislator has introduced a provision that struck a balance in favor of privacy by preemptively restricting access to content pending the verification of its accuracy. However, the chilling effects on freedom of expression should be limited. First, this is a narrower—and an intrinsically different—scenario than the right to be forgotten or erasure as it applies only to cases where the accuracy of the personal data is contested. Second, the access restriction to data whose accuracy is challenged should be quite brief. According to the GDPR, the restriction should be lifted as soon as the data controllers perform the verification of the accuracy of data.[58] This should happen in the same time range as the RTBF requests' processing time, which has been increasingly reduced in the last two years to less than 20 days per request.[59]

### *3.2. Implementing European Guidelines in National Courts*

Meanwhile, European national courts and authorities gave specific implementation to the ECJ decision by operating the necessary balancing of rights between personal privacy interest and public interest in freedom of expression and access to information. The Court of Amsterdam narrowed the ECJ's test by stating that the *Google Spain* ruling "does not intend to protect individuals against all negative communications on the Internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily

---

[53] GDPR, *supra* note 5, at Art. 17.

[54] *Id*., at Art. 17(3) (d); *see also* Art. 89(1).

[55] *See* DP Directive, *supra* note 10, at Art. 9.

[56] *Id*., at Art. 85; *see also* Preamble, Recital 153 (noting that "[t]his should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries" and that "[i] In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly").

[57] *See* GDPR, *supra* note 5, at Art. 18(1) (a).

[58] *Id*.

[59] *See* Gerg Sterling, Report: 2 Years in, 75 Percent of Right to Be Forgotten Asks Denied by Google, Search Engine Land, May 12, 2016, http://searchengineland.com/report-2-years-75-percent-right-forgotten-asks-denied-google-249424.

defamatory' expressions."[60] That decision dealt with an escort agency owner who wanted links to his criminal history removed from Google. Google refused to comply fully with this request. The suit sought a court order for Google to remove all search results referring to his conviction. In handing down its decision, the Court of Amsterdam made clear that privacy should prevail over freedom of speech and information.[61] The Court stressed that a person convicted for a serious crime will hardly meet the criteria that the communication is irrelevant, excessive, and unnecessarily defamatory and argued that the conviction for a serious crime, and the negative publicity as a consequence thereof, in general provide information about an individual that will remain relevant.[62] The criteria of "irrelevant, excessive, and unnecessarily defamatory" may be met only in very exceptional circumstances, "for instance when the offense committed is brought up again without a clear reason, apparently for no other purpose than to damage the individual involved, if reporting is not factual but rather a 'slanging-match.'"[63]

Shortly after the Amsterdam ruling, the Italian Privacy Authority reinforced the point that the RTBF must be balanced with freedom of the press. On March 31, 2015, the Italian Privacy Authority issued a decision stating that users cannot obtain the delisting of search results of recent news with a relevant public interest.[64] Search engines must delete or edit automatically generated snippets accompanying the search results if they are misleading.[65] The claimant contested Google's decision not to delist a news article referring to a judicial inquiry in which the claimant was involved. The claimant argued that the news article was "extremely misleading and strongly detrimental."[66] The Authority denied the delisting request upon the finding that the news was extremely recent.[67] Additionally, the Authority highlighted the relevant public interest of the news, which referred to an important judicial inquiry with the involvement of a large number of people at the local level.[68] For all these reasons, the Authority found that the freedom of

---

[60] Rechtbank [District Court] Amsterdam, 18 September 2014, ECLI:NL:RBAMS:2014:6118 as translated in Joran Spauwen and Jens van den Brink, Dutch Google Spain ruling: More Freedom of Speech, Less Right To Be Forgotten For Criminals, Inforrm's Blog, September 27, 2014, https://inforrm.wordpress.com/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink; Gerechtshof [Court of Appeal] Amsterdam, March 31, 2015, ECLI:NL:GHAMS:2015:1123 (confirming the District Court decision); *see also* Rechtbank [District Court] Amsterdam, February 13, 2015, ECLI:NL:RBAMS:2015:716 (discussing a request from a partner in a consultancy firm to delist from searches under his name an article that reported on a lawsuit he was involved about two years before); Stefan Kulk and Frederik Z. Borgesius, Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain', 2 EUROPEAN DATA PROTECTION L. REV. 113 (2015), *available at* http://edpl.lexxion.eu/article/EDPL/2015/2/5 (examining how the Google Spain judgment has been applied in the two Dutch cases above).

[61] Gerechtshof Amsterdam, as cited in Spauwen and van den Brink, *supra* note 60..

[62] *Id*.

[63] *Id*., as translated in Spauwen and van den Brink, *supra* note 60.

[64] *See* Garante per la Protezione dei Dati Personali [Data Protection Authority], Decision No. 618, December 18, 2014, http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/3736353 [Italian only].

[65] *Id*.

[66] *Id*.

[67] *Id*.

[68] *Id*.

the press should prevail on the right to be forgotten under the present circumstances.[69] If the interested party deems the news to be false, he may ask the publisher to update, rectify or integrate the article. The Authority also concluded that search engines must delete or modify the automatically generated snippets summarizing the information included in the search results if they are misleading.[70] Actually, in this case the summary did not match the facts described in the news article and associated the claimant to more serious crimes than those for which he was under investigation.[71]

In Italy, further clarifications on the necessary balance between the RTBF and FoE came from a December 2015 decision of the Tribunal of Rome. The Roman Court noted that a well-known attorney who was involved in alleged illicit activities from 2012 to 2013 together with religious figures and known Roman criminals had no right to seek the delisting of fourteen URLs referring to those events.[72] The Court, construing the notion of public figure and public role in an inclusive manner, reinforced the understanding that Google Spain implies that no RTBF can be claimed for recent data of public interest.[73] In addition, any claim against the defamatory nature of the information should be brought against the third party websites publishing the untruthful or obsolete news, rather than the search engine.[74]

The Belgian *Cour de Cassation* (the highest national court) has also ruled on the RTBF.[75] There the case did not involve delisting from Google search engine—or intermediary liability—but rather shed light on whether the RTBF should prevail over freedom of expression in records included in newspapers' archives. The Belgian newspaper *Le Soir* made its entire archive freely available online in 2008.[76] It included a 1994 article reporting of a car accident in which two people died. The driver's full name was mentioned in the article and requested *le Soir* to remove the article or anonymize it.[77] The Belgian *Cour de Cassation* made specific reference to *Google Spain* and decided that the right to privacy—embedding the RTBF—might justify under specific circumstances the limitation of *Le Soir*'s right to freedom of expression.[78] The Court clarified that *Le Soir*'s liability—and prevalence of the RTBF over FoE—would be justified by the relevant lapse in time, lack of actual interest in communicating the name of the driver, and the circumstance that the anonymization does not have an impact on the essence of

---

[69] *Id*.

[70] *Id*..

[71] *Id*.

[72] *See* Google v. XXX, No. 23771 (Rome Tribunal, December 3, 2015)

[73] *Id*.

[74] *Id*.

[75] *See* P.H. v. O.G., C.15.0052.F (Belgian Supreme Court [Cour de Cassation], April 29, 2016), *available at* http://www.juricaf.org/arret/BELGIQUE-COURDECASSATION-20160429-C150052F (French only).

[76] *Id*., Motifs: 1.

[77] *Id*.

[78] *Id*., Motifs: 4.

the information.[79] Therefore, Le Soir was requested to remove the name of the applicant from the article in its database.

Another decision from the Italian *Corte di Cassazione* (Italy's Supreme Court) clarified the matter of the right to be forgotten in public registries.[80] The case dealt with data protection and the processing of personal information provided by the Italian Commercial Register. The court finally referred the question of whether the rational of the RTBF can be also applied to information available in public registries to the European Court of Justice for further clarifications.[81] Pending a decision from the ECJ, the Advocate General—providing non-binding opinions on cases under review before the ECJ—issued conclusions that followed in the footsteps of the preliminary findings included in the Italian Supreme Court's referral. The Advocate General concluded no RTBF can be applied to data in public registries if there is a prevalent public interest. In particular, the personal data included in the Commercial Registry "cannot be cancelled, anonymized, or blocked, or made available only to a limited number of interested parties," given the prevalent interest in promoting market transparency and protecting third parties.[82]

In October 2015, Costeja himself apparently lost his right to be forgotten. The Spanish DP Authority denied the right to suppress links to comments about that case. [83] Given the relevance of the CJEU's ruling, comments discussing the case and the facts behind it

---

[79] *Id*., Motifs: 6-9. The Italian Corte di Cassazione [Supreme Court] came down multiple times to similar conclusion, noting that publishing old news—forgotten or unknown to the public—that may damage an individual's personal identity should be rated as a violation to the right to oblivion. *See* Decision N. 3679 (Corte di Cassazione, 1998). According to the Italian Supreme Court, if there is no actual interest in the publication of a relevant public news, individuals enjoy the right to have their personal events forgotten by the public. *See* Decision No. 16111 (Corte di Cassazione, 2013).

[80] Camera di Commercio Industria Artigianato Agricoltura di Lecce v. S.M, No. 15096 (Corte di Cassazione [Supreme Court], July 17, 2015) (Italian only); *see also* Alessandro Mantelero, Right to be Forgotten e Publici Registri. I Giudici Italiani Chiedono Lumi alla Corte di Giustizia, ma Lasciano Poche Possibilità al Diritto alla Cancellazione dei Dati, 1 Giurispridenza Italiana Commentata 70 (2016), *available at* https://www.researchgate.net/publication/299469994_Right_to_be_forgotten_e_pubblici_registri_I_giudici_italiani_chiedono_lumi_alla_Corte_di_Giustizia_ma_lasciano_poche_possibilita_al_diritto_alla_cancellazione_dei_dati (Italian only).

[81] Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, C-398/15 (European Court of Justice) (request for a preliminary ruling lodged on July 23, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=170468&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=549071; *see also* Alessandro Mantelero, Right to be Forgotten and Public Registries. A Request to the European Court of Justice for a Preliminary Ruling, 2 European Data Protection Law Review (forthcoming, 2016), *available at* http://ssrn.com/abstract=2795895.

[82] See Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, C-398/15 (European Court of Justice, September 8, 2016) (AG Opinion), *available at* http://curia.europa.eu/juris/celex.jsf?celex=62015CC0398&lang1=en&type=TXT&ancre.

[83] Agencia Espanola de Protección de Datos, Resolution N. R/02179/2015 (October 2015) (Spanish only) [hereinafter Spanish DPA N. R/02179/2015]; *see also* Miquel Peguera, No More Right-to-be –Forgotten for Mr. Costeja, says Spanish Data Protection Authority, CIS Blog, October 3, 2015, http://cyberlaw.stanford.edu/blog/2015/10/no-more-right-be-forgotten-mr-costeja-says-spanish-data-protection-authority.

must be considered of public interest, according to the DPA's decision.[84] As soon as Mr. Costeja became a public figure he lost his right to be forgotten. In a perfect Streisand effect scenario,[85] the wide publicity of the *Google Spain* decision frustrated Costeja's attempt to hide the information included in the links finally delisted. Costeja was often depicted in the media as the man who won the *Google Spain* case but also attracted negative comments. [86]When asked to remove one of such comments—most likely, a blog post tiled "The Unforgettable Story of the Seizure to the Defaulter Mario Costeja González that Happened in 1998," featuring as the first results in Google.es for Costeja's name search—Google refused.[87] Ultimately the Spanish DPA dismissed the claim that Costeja brought against Google.[88] The Spanish DPA distinguished the case from the ECJ *Google Spain* decision because there is a preponderant public interest to get informed regarding a well-known ECJ case.[89] The ECJ also noted that Mr. Costeja himself went public with the details that he now wants to be removed from public attention, therefore losing his right to be forgotten also on that account.[90]

Meanwhile, Spanish courts further qualified online platforms' liability in connection to the right to be forgotten. In a civil lawsuit brought to seek damages for an untimely removal, the Court of Appeal of Barcelona made clear that Google was supposed to pay damages from the very moment it obtained actual knowledge of the offending links up to the removal of the links.[91] According to the court, Google lost its safe harbor protection when it obtained actual knowledge of the offending links, which occurred at the time Google was notified of the DPA decision that initially ordered to remove the links.[92] In this instance, damages arise from the application of the Data Protection Directive ordering Member States to "provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered."[93]

In line with the WP29 Guidelines, the national application of the right to be forgotten in Europe moved forward by implementing strong safeguards for freedom of expression and public interest. In addition, the GDPR specifically includes exemptions, safeguarding

---

[84] *Id*.

[85] *See* Streisand Effect, Wikipedia, https://en.wikipedia.org/wiki/Streisand_effect.

[86] *See* Peguera, *supra* note 83.

[87] *Id*. (implying that that should be the comment, although not specifically mentioned by the Spanish DPA decision).

[88] *See* Spanish DPA N. R/02179/2015, *supra* note 84, at 12.

[89] *Id*., at 10-11.

[90] *Id*.

[91] *See* Google Spain et al v. Don Domingo, No. 364/2014 (Barcelona Court of Appeals, July 17, 2014) (Spanish only) [hereinafter, Google Spain v. Don Domingo] (discussing damages for the removal of links—that appeared following a claimant name's search on Google—to the Official Gazette of a 1991 pardoned criminal conviction for violating "public health" regulation); *see also* Miquel Peguera, Right to be Forgotten: Google Sentenced to Pay Damages in Spain, CIS Blog, October 14, 2014, http://cyberlaw.stanford.edu/blog/2014/10/right-be-forgotten-google-sentenced-pay-damages-spain.

[92] See Google Spain v. Don Domingo, *supra* note 91.

[93] *See* DP Directive, *supra* note 10, Art. 23.

the fundamental right to freedom of expression.[94] However, heated debate has ensued in other countries, most prominently Germany. German commentators—including a Supreme Court judge—expressed "serious concerns" about the ECJ's emphasis on extended intermediary liability and the ECJ's finding that the right to be forgotten "override[s], as a rule, not only the economic interest of the operator of the search engine *but also the interest of the general public*."[95] However, German courts consistently applied the Google Spain ruling. The District Court of Heidelberg referred to the ECJ ruling when ordering Google to remove links to a web page, which claimed to "expose" racists and awarding damages for the company's failure to remove the links promptly upon notification.[96] On November 7, 2014, the District Court of Hamburg similarly ordered Google to remove search results that suggested that the plaintiff had owned a brothel.[97]

### *3.3. Limited Chilling Effects in a Privately-Enforced Right to Be Forgotten*

Under the ECJ ruling, OSPs might have a responsibility to assess each de-listing request on a case-by-case basis. In truth, it should be noted at the outset that the ECJ indicated to a judicial body—the Spanish Superior Court—the criteria to be followed when balancing the right to privacy with other fundamental rights, rather than a private party such as Google. Nonetheless—to limit liability risks—Google adopted a proactive approach and made preliminary determinations on the de-linking requests based on the criteria outlined in the ruling.[98] The role of online search engines becomes the most controversial question of the implementation of the right to be forgotten. Indeed, the power of making decisions that might trample on fundamental rights shifts from judicial authorities to private parties.[99] In particular, as Taddeo and Floridi argue, this ruling, "puts OSPs in the position to have to decide about those criteria and those principles and their implementation. Hence, OSPs become both the judge and the jury."[100] Although these rulings undeniably strengthen a tendency in privatization of judging power online,[101] it might be argued, however—in contrast to Taddeo and Floridi conclusions—that actually all criteria and principles necessary for a balanced implementation of the right to be forgotten have been defined quite in detail by European regulatory and judicial institutions.

---

[94] *See* GDPR, *supra* note 5, at Art. 17(1) and 80.

[95] *See* Johannes Masing, Justice of the German Federal Constitutional Court, Preliminary Assessment of the Google Decision of the ECJ, Verfassungblog, August 14, 2014, http://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/#.VLRgNivF9EJ;

[96] *See*, Google v. XXX, 2 O 162/13 (Landgericht Heidelberg [District Court of Heidelberg], December 9, 2014), *available at* http://cyberlaw.stanford.edu/page/wilmap-germany.

[97] *See* Google v. WFM, 324 O 660/12 (Landgericht Hamburg [District Court of Hamburg], November 7, 2014), *available at* http://cyberlaw.stanford.edu/page/wilmap-germany.

[98] *See* The Advisory Council to Google on the Right to be Forgotten, https://www.google.com/advisorycouncil.

[99] *See* Rosen, *supra* note 21, at 88.

[100] Taddeo and Floridi, *supra* note 4, at 20.

[101] *See* Felicity Gerry and Nadya Berova, *The Rule of Law Online: Treating Data like the Sale of Goods: Lessons for the Internet from OECD and CISG and Sacking Google as the Regulator*, 30(5) COMPUTER L. & SECURITY REV. 465, 465–481 (2014); see also infra, at 92.

The data show a limited chilling effect of the RTBF because in practice ungrounded RTBF requests have been largely rejected. According to a report compiling aggregate data on the RTBF, in two years, Google denied seventy-five percent of RTBF requests.[102] Again, Google internal statistics showed that ninety-five percent of Google privacy request are from citizens seeking to protect personal and private information, and only five percent of requests required de-linking in relation to criminal activities or public figures.[103] In addition, requests' processing time has radically improved in the last two years from 49 days in 2015 to 20 or less days per request in 2017.[104] This shows that major search engines have the technical capabilities to efficiently start the review process. The data also show that search engines process RTBF requests by erring, if it is the case, in minimizing chilling effects, rather than over removing. There exists an argument against the RTBF that states minor players would not have the same capabilities and therefore would err in blindly delisting without appropriate prior scrutiny and review. This argument, however, would be hardly sustainable in light of the principle of proportionality and the necessary balancing of interests at stake that the ECJ—and national courts—are called to make.[105] Data controllers with the technical capabilities to do so according to public interest will deal almost the entirety of the requests.[106]At the outset, in any event, it should be given very little merit to the argument that courts should not apply the necessary balancing of rights—according to EU Directives and national Constitutions—because of limited technical means of those called upon enforcing court orders.

In any event, there might be alternatives to delegating pre-screening of RTBF requests to private parties. One might entail the creation of a public body that would serve as a centralized EU-wide clearinghouse and should review delisting requests and decide upon them according to institutional guidelines and human rights' frameworks.[107] This body could be created under the aegis of Article 29, for example. Alternatively, as was recently proposed in France, an Internet ombudsman could be instated with the goal to safeguard

---

[102] *See* Gerg Sterling, *supra* at 59; *see also* Google Transparency Report, https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en (accessed January 5, 2017) (stating that Google removed 43.2% of the 1,846,066 URLs evaluated for removal).

[103] *See* Sylvia Tippmann and Julia Powles, Google Accidentally Reveals Data on 'Right to be Forgotten' Requests, The Guardian, July 14, 2015, https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests.

[104] *See* Gerg Sterling, *supra* at 59.

[105] *See* Julia Powles, *The Case that Won't be Forgotten*, 47 LOYOLA U. CHI. L. J. 583 (2015) (noting that suggested that if Google was really concerned about smaller players, it would look seriously at creating an independent, industry-sponsored platform to do this job).

[106] *See* Desktop Search Engine Market Share, https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0 (other—not major IT companies—search engines amount to less than 1%); Mobile/Tablet Search Engine Market Share, https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=1.

[107] *See* Martin Husovec, Should we Centralize the Right to Be Forgotten Clearing House?, CIS Blog, May 30, 2014, https://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house.

free speech.[108] According to a bill recently introduced in the French Senate, the role of the ombudsman would be to supervise and provide "a content qualification assessment procedure" to help online service providers prevent online over-zealous removal of online materials by regulating online complaints.[109]

## 4. It's Not About Deleting Content, but Processing Name Searches

There are other factoids pertaining to the scope of the right that should perhaps be debunked as well.[110] The *Costeja* decision is not about information being suppressed from the Internet. According to the WP29 Guidelines, the original information will always remain accessible and no information is deleted from the original source. The right only affects the results obtained from searches made on the basis of a person's name. That is, the original information will still be accessible using other search terms, or by direct access to the source.[111] A ruling from the UK Information Commissioner's Office in August 2015 clarified this point as well:

> Let's be clear. We understand that links being removed as a result of this court ruling is something that newspapers want to write about. And we understand that people need to be able to find these stories through search engines like Google. But that does not need them to be revealed when searching on the original complainant's name.[112]

Data protection law does not give me the right to ask YouTube to delete a video of me you uploaded; but it does give me the right to ask, and not force, Google to stop referring to that video when people enter my name in the search bar.

## 5. It Is Not About Intermediaries, but Data Controllers

The right to be forgotten applies to data controllers, not intermediaries. Whether search engines—or platforms like YouTube, Facebook, Twitter—would be considered data controllers for the purposes of data protection law or intermediaries for the purposes of the eCommerce Directive entirely depends on the operations they perform. This seems like Article 29 *Opinion on the Concepts of 'Controller' and Processor'*, which states that

---

[108] *See* France Plans Internet Ombudsman to Safeguard Free Speech, The Guardian, December 19, 2016, https://www.theguardian.com/technology/2016/dec/19/france-plans-internet-ombudsman-to-safeguard-free-speech

[109] *See* Proposition de Loi No. 151, portant création d'un Ombudsman compétent pour qualifier le contenu sur l'internet de licite ou illicite (November 25, 2016), http://www.senat.fr/leg/ppl16-151.html.

[110] *See*, *e.g.*, Mark Bergen, Google Ordered to Forget 'Right to Be Forgotten' Stories, Recode, August 20, 2015, http://recode.net/2015/08/20/google-ordered-to-forget-right-to-be-forgotten-stories (for spreading false assumptions in a sensationalistic fashion).

[111] *See* WP29 Guidelines, *supra* note 47, at 2.

[112] ICO Orders Removal of Google Search Results, ICO, August 20, 2015 (statement from Deputy Commissioner David Smith), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/08/ico-orders-removal-of-google-search-results; *see also* Data Protection Act 1998, Supervisory Powers of the Information Commissioner, Enforcement Notice to Google Inc. (August 18, 2015), https://ico.org.uk/media/action-weve-taken/enforcement-notices/1560072/google-inc-enforcement-notice-102015.pdf.

an Internet service provider of hosting services "is in principle a processor for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. *If however, the ISP further processes for its own purposes the data contained on the websites then it is the data controller with regard to that specific processing*."[113] Again, Recital 14 of the eCommerce Directive reinforces this functional distinction and says "the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries."[114] Intermediaries are governed by data protection law under its own terms—and the eCommerce Directive does not regulate—and exempt—them as far as data protection obligations are concerned. Reciprocally, the General Data Protection Regulation will function "without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive."[115]

In *Google Spain*, the European Court of Justice distinguished between specific activities by differentiating the decision to publish information from the decision to refer to that information on the basis of a name search. This specific decision in organizing and aggregating information has substantial effects impinging on users' privacy rights online. According to the court, users who carry out searches on the basis of an individual's name are able to obtain "a structured overview of the information relating to that individual that can be found on the Internet enabling them to *establish a more or less detailed profile of the data subject*."[116] This specific, autonomous action of linking a search term with a search result becomes relevant for data protection purposes and—when this linking appears "irrelevant, inadequate, or excessive"—the search engine can be held responsible under data protection law.

Another example of this functional distinction comes from a decision of the Spanish National High Court confirming that intermediaries are not specifically affected by the right to be forgotten. The Court ruled that in the case of user-generated platforms (such as Blogger) the responsibility of data processing is not applied to Google but the blog owner. As a result, Google could not be ordered to remove content directly but only delist it from name search results.[117] The court made a distinction between a hosting platform

---

[113] *See* Article 29 Data Protection Working Party, Opinion on the Concepts of 'Controller' and Processor', 00264/10/EN WP 169, at 25, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (emphasis added).

[114] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 O.J. (L 178) 1-16, at Recital 14, *available at* http://cyberlaw.stanford.edu/page/wilmap-european-union [hereinafter eCommerce Directive].

[115] *See* GDPR, *supra* note 5at Art. 2(3).

[116] Google Spain, *supra* note 1, at § 37 (emphasis added).

[117] *See* Google Spain, SL v. Agencia Protección de Datos, No. 70/2015 (National High Court, March 2015) (reversing a DPA and a first instance decision); *see also* Agencia Espanola de Protección de Datos, Resolution N. R/01509/2010 (July 2010) (Spanish only) (originally ordering Google to remove personally identifiable information from a blog hosted on Blogger that included information about a crime the claimant committed many years before, although Google was not liable for the content of the blog as it was protected by the hosting exemption); Miquel Peguera, Spain: The Right to Be Forgotten Does not Apply to

and a search engine. Actually, in the same ruling, Google as a search engine was deemed controller and ordered to delist the search result.[118] This case confirms that intermediaries are not specifically affected by the right to be forgotten. Data protection laws do not apply to intermediaries as such but data controllers.

According to *Google Spain* and EU law, a functional distinction can be made between different operations of online intermediaries, each coming with their own exemptions and liabilities. As Van Eecke describes:

> [a]t the outset, it is important to note that the protection of the eCommerce Directive is situated at the service level (or at the sub-service level), and not at the company level. As a result, a single company can at the same time act as a mere conduit, caching and/or hosting provider. Any questions regarding liability or injunctions must be assessed by taking into account the specific service considered.[119]

Liability exemptions apply only to activities, not entire services. Therefore, exonerating entities from liability over third-party content or activities, does not make them immune for what they autonomously decide to do with the information, especially when activities of online service providers increasingly extend into actively processing the information they host or transmit for a variety of different purposes. Basically, intermediaries performing activities as data controllers (e.g. processing data for their own purposes) will be bound by data protection obligations and never qualify as neutral enough to escape those obligations. In contrast, intermediaries which do not qualifies as data controllers can never be stripped of their liability exemptions for any infringement arising from data protection obligations. Duties and rights in data protection law are applicable against controllers; and intermediaries, due to a progressive complexification of their activities, are increasingly wearing different hats, each coming with its own responsibilities.

## 6. Extra-Territorial Application of the Right to Be Forgotten

The extraterritorial application of the right to be forgotten remain perhaps the thorniest issue to be dealt with in the implementation of the right. It is a problem inherent with acting on search engines to block access to content online, which makes impossible to obtain perfect enforcement. As Professor Floridi puts it:

> Yet I fear that, in an infosphere that does not know geographical boundaries, acting on search engines to block access to contents is never going to be the ultimate solution. If some content is harmful, it should be blocked at the source, for any search engine, anywhere, or removed completely, as we do with child pornography. Only this would be an effective implementation of the right to be forgotten.[120]

European institutions endorse the view that delisting should have an extra-territorial reach. On the territorial effect of de-listing decisions, the WP29 guidelines noted that

---

Blogger, CIS Blog, March 4, 2015, https://cyberlaw.stanford.edu/blog/2015/03/spain-right-be-forgotten-does-not-apply-blogger.

[118] *Id*.

[119] Peter Van Eecke, *Online Service Providers and Liability: a Plea for a Balanced Approach*, 5 COMMON MARKET L. REV. 1462

[120] We dislike the truth and love to be fooled (Luciano Floridi), CYCEON, November 21, 2016, https://cyceon.com/2016/11/21/luciano-floridi-oxford-uk-google-interview.

limiting de-listing to EU domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, "this means that in any case *de-listing should also be effective on all relevant .com domains*."[121]

In accordance with the WP29 Guidelines, the *Commission Nationale de l'informatique et des Libertés* (CNiL), the French data protection authority, ordered Google to apply the RTBF on all domain names of Google's search engine, including the .com domain.[122] As many other national data protection authorities in Europe, the CNil supervises the application of the ECJ's judgment on the RTBF in case of refusal by the search engines to carry out the requested delisting. In response to hundreds of individual complaints since the *Google Spain* decision, the CNil requested Google to delist search results in multiple occasions.[123] In all those instances, the CNiL expressly requested that the delisting had to be effective across the whole search engine, regardless of the domain extension through which the users access the information.[124] However, initially, Google applied the delisting only to European extensions of its search engine. RTBF infringing search results still remained accessible in the French territory from google.com and other non-European extensions.[125]

Google proposed solution was geo-localization.[126] Google extended the removal of the URLs to any domain-based version of its search engine used by anyone conducting name-based searches from the same European country as the original approved request. If a French resident successfully requests Google to remove a search result under queries for their name, the link will not be visible on any version of Google's website, including Google.com, when the search engine is accessed from France. Google will use the browser's IP address to determine their location. However, the CNiL deemed this development insufficient to protect French users' rights. In imposing a €100,000 fine on Google, the CNiL Restricted Committee, noted that:

> the right to be delisted is derived from the right to privacy, which is a universally recognized fundamental right laid down in international human rights law. Only delisting on all of the search engine's extensions, regardless of the extension used or the geographic origin of the person performing the search, can effectively uphold this right. The solution that consists in varying the respect for people's rights on the basis of the geographic origin of those viewing the search results does not give people effective, full protection of their right to be delisted.[127]

According to the CNiL, the RTBF is absolute and French institutions must protect it as long as the infringement of the right causes damages to French citizens. As the CNiL

---

[121] WP29 Guidelines, *supra* note 47, at 3 (emphasis added).

[122] *See* CNiL Orders Google to Apply Delisting on All Domain Names of the Search Engine, CNiL, June 12, 2015, https://www.cnil.fr/fr/node/15790.

[123] *Id*.

[124] *Id*.

[125] *Id*.

[126] *Id*.

[127] CNiL, Restricted Committee, Decision No. 2016-054 (March 10, 2016), https://www.cnil.fr/sites/default/files/atoms/files/d2016-054_penalty_google.pdf.

explains, contacts living outside Europe can still access the delisted search result linking to content that may infringe the privacy of the person concerned; contacts living in Europe and using a non-European search engine extension, such as '.com', with a non-French IP address can still access the delisted search result; finally, certain technical solutions can easily get around Google's filtering system by allowing Internet users to change the geographic origin of their IP address.[128] If Google maintains a subsidiary in France it will be liable for not doing so. The option remains only to comply with CNiL requests or stop providing services in France.

*CNiL v. Google* is currently before the French Court that will review CNiL's extraterritorial claims. On December 9, 2016, Google's Global Privacy Counsel, Peter Fleischer, published a blog post reasserting the company's position regarding the CNiL case. Google believes that de-indexing content worldwide to comply with one country's rules and decisions would hinder freedom of expression:

> What if links to stories about someone's past—stories about defrauding an international business or about medical tourism malpractice—were removed from Google search in your country, not because of your local laws but because someone was able to use the laws of another country. How would you feel about that? [. . .] The right to be forgotten can sometimes seem complex, and discussions about jurisdiction online certainly are complicated. But this issue is simple: should the balance between the right to free expression and the right to privacy be struck by each country—based on its culture, its traditions, its courts—or should one view apply for all?[129]

These are perhaps over-simplistic statements. On the matter of extraterritoriality, CNiL specifically noted "this decision does not show any willingness on the part of the CNiL to apply French law extraterritorially. It simply requests full observance of European legislation by non European players offering their services in Europe."[130] A few points might be helpful to clarify this position. First, there is no other country than France where French law is supposed to apply. There are Internet domains where French law would apply, as Google argues: "[u]ltimately, we might have to implement French standards on Google search sites from Australia (google.com.au) to Zambia (google.co.zm) and everywhere in between."[131] The disconnection lies with a misperception regarding the nature of the Internet. Digital domains are just fictional worlds unsanctioned by international rules defining national sovereignty. The Westphalian sovereignty system can be hardly stretched to reach the Internet.[132] Google.com.au is not Australia, google.co.zm is not Zambia—and countries around the world are little inclined to cope longer with google.com being a U.S. protectorate. As the

---

[128] *Id*.

[129] Peter Fleisher, Reflecting on the Right to be Forgotten, Google Blog, December 9, 2016, https://blog.google/topics/google-europe/reflecting-right-be-forgotten; *see also* Daphne Keller, Global Right to be Forgotten: Why CNiL is Wrong, CIS Blog, November 18, 2016, https://cyberlaw.stanford.edu/blog/2016/11/global-right-be-forgotten-delisting-why-cnil-wrong.

[130] CNiL, Right to Delisting: Google Informal Appeal Rejected, September 21, 2015, https://www.cnil.fr/fr/node/15814.

[131] Fleisher, *supra* note 129 (emphasis added).

[132] *See* Chris Demchak and Peter Dombrowski, *Cyber Westphalia: Asserting State Prerogatives in Cyberspace*, 7 GEORGETOWN J. INT'L AFFAIRS 29, 33 (2015) (noting that "the process of establishing cyber borders and thus states' sovereignty will be nonlinear, dangerous, and lengthy.")

Internet has yet to be partitioned in digital territories under the jurisdiction of a specific country, there is no reason to think that French rules should not apply to French data subjects when roaming any digital domain other than google.fr or google.eu.

A second key point to emphasize is that the laws of the data subject shall impose the removal, rather than merely the "laws of another country." The Article 29 Guidelines clarified that the right to be forgotten should apply, *ratione personae*, only to requests originating from Europe:

> Article 8 of the European Charter of Fundamental Rights [. . .] recognises the right to data protection to "everyone." In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State."[133]

Google's question "should the balance between the right to free expression and the right to privacy be struck by each country—based on its culture, its traditions, its courts—or should one view apply for all?" is misleading. The correct question to ask would be whether the balance between the right to free expression and the right to privacy should be struck by the laws of the country of citizenship of the data subject. Do Internet users around the world have a right to seek information regarding a French citizen—or resident—that French law banned from further disclosure? According to CNiL position, I would suggest, there's no "one view applying for all" but the view of the country of citizenship applying to their own citizens regardless of the digital domain where their rights might be violated. The alternative would be to leave those fundamental rights unattended when they occur to be infringed in a digital domain supposedly out of reach of national enforcement. CNiL position does stress that the Internet is not set in a bubble suspended in a perfect vacuum with no accountability for individual rights granted by French law—*even* for sake of an amorphous, unqualified reference to freedom of expression. There are physical persons behind each name search, each suffering very real damages. As long as they are located in France they will enjoy protection under French law no matter where their digital endeavors take them. According to the CNiL, our citizenship—and the rights that it portends---follows us everywhere in the digital environment. Hiding in a fictitious reality does not suffice to escape the reach of national law as long as a party does business in that country.

This interpretation would be in line with the International Covenant on Civil and Political Rights that provide "an effective remedy" to any person whose rights and freedoms—including the right to privacy—are violated.[134] The Covenant also provides that signatories undertakes to "ensure to all individuals within its territory and subject to its jurisdictions the rights recognized in the [. . .] in the Covenant."[135] According to Professor Dan Svantesson, this would imply that the signatories of the Covenant are under an obligation "to provide legal protection against unlawful attacks on the privacy

---

[133] WP29 Guidelines, *supra* note 47, at § 19.

[134] United Nations Organization, International Covenant on Civil and Political Rights, March 23, 1976, Art. 3 and 17, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx#.

[135] *Id*., at Art. 2.

of the people subject to its jurisdiction and those present within its territory, regardless of the origin of the attack."[136]

The CNiL's arguments fit within some of the traditional principles used for establishing extraterritorial jurisdiction. They resemble closely the passive personality principle and the effects theory. According to the passive personality principle or nationality principle, States can claim jurisdiction over offences to their nationals committed abroad.[137] Alternatively, according to the effects theory, a State can exercise its jurisdiction in its own territory over a foreign national for conducts that took place abroad and produce effects within its territory.[138]

Finally, the statement that the CNiL standard would lead to a race to the bottom should also be dispelled. As it is argued, if CNiL approach were to be embraced as a standard for internet regulation, "[i]n the end, the Internet would only be as free as the world's least free place." [139] But is this true? Probably, not. Actually, the Internet would only be as free as the world. It will mirror exactly the world as it is. In light of the CNiL—and EU—approach, data subjects would enjoy rights everywhere in the Internet according to the rights they enjoy in their own jurisdiction.

## 7. Conclusions

As the RTBF unfolded over the last two years it has become increasingly clear that there has been much ado about nothing. The RTBF is a long-standing right of EU citizens rooted in the doctrine of informational self-determination. *Google Spain* enforced this right against search engines as they were found to be acting as data controllers. Since May 2014, European institutions and courts have been looking for a fine tuned equilibrium between the RTBF and FoE. To put it bluntly, FoE remains untouched as the RTBF does not apply to newsworthy information and public figures, de-linked content still remain published in its original Internet location, and a different query will still lead to that content. RTBF did not impact journalism[140] and "there is no room for concern for archives and for the right to remember given the restricted application of RTBF."[141] The myth that the RTBF hurts FoE should be displaced once for all. It is in the nature of privacy rights to constrict FoE. The right to be forgotten—or delisted—does not encumber FoE in any different way than the traditional privacy/FoE dichotomy used to do under European law. If any, more safeguards have been added—or at least clearly spelled out—to reconcile the right to privacy with FoE.

---

[136] Dan Svantesson, *The Extraterritoriality of EU Data Privacy Laws – Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, 50(1) STANFORD J. INT'L L. 53, 78 (2014); see also PEROTTI, *supra* note 27, at 31.

[137] *Id*., at 18.

[138] *See* S.S. Lotus (France v. Turkey), 1927 P.C.I.J. (ser. A) No. 10 (September 7, 1927), at 19, *available at* http://documents.law.yale.edu/sites/default/files/SS%20Lotus%20-%20PCIJ%20-%201927.pdf.

[139] Peter Fleischer, Implementing a European, not Global, Right to be Forgotten, July 30, 2015, https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html.

[140] *See* Perotti, *supra* note 27.

[141] Melanie Dulong de Rosnay and Andres Guadamuz, Memory Hole or Right to Delist: Implications of the Right to be Forgotten for Web Archiving, 6 Reset [Online] (2016), http://reset.revues.org/807.

Entrusting private parties with the adjudication—although preliminary—of requests that might entail the necessary balancing of counterpoising fundamental rights still remain one negative connotations of the present implementation of the RTBF. This balancing should be preferably left to courts or other state authorities. Nonetheless, data show very limited chilling effects in the adjudication process performed by search engines. Major search engines proved to have technical and organizational capabilities to address requests effectively and promptly. In any event, proposal—such as national or super-national clearing houses or FoE ombudsman—have been discussed and could be readily implemented to mitigate the negative externalities of private enforcement.

The idea that extra-territorial application of the RTBF might unleash a kraken that can break down the Internet should be contextualized within the present political scenario. The extra-territorial application of the RTBF follows in the footsteps of a global move towards data protectionism against the *de facto* market dominance of U.S. Internet conglomerates.[142] As a recent article on Slate has argued, "it's hard to completely share America's enthusiasm for the same internet everywhere, when that internet happens to be so utterly dominated by U.S. firms." The rest of the world may fear—Slate continues—that "the internet is explicitly used by the U.S. State Department to preach for American values and interests abroad."[143] Google might reinforce these fears—as it pleads against the CNiL decision—putting forward arguments such as "any such precedent [of having to implement French standards everywhere] would open the door to countries around the world, *including non-democratic countries*, to demand the same global power."[144] This is exactly the rhetoric that summons data protectionism from its grave. It leads to believe that for those "non-democratic countries"—and possibly other non-democratic "enough," including actually also France and Europe—companies operating the Internet should serve as guardians of the world citizens' rights online according to the laws and values of the country where these companies are incorporated.

The idea that there might be countries better suited than other to check and balance individual rights is certainly insufferable–and inherently tainted by relativistic fallacies. This rhetoric is also untenable in light of the principles of self-determination and mutual respect that should govern international relationships—and are actually at the core of the Westphalian arrangement. Against this rhetoric, world countries increasingly seek control

---

[142] *See, e.g.*, *Schrems v. Data Protection Commissioner*, C-362/14, (European Court of Justice, October 6, 2015); *see also* Global Freedom of Expression, Columbia University, Schrems v. Data Protection Commissioner, https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner; CNiL, The French Data Protection Authority Publicly Issues Formal Notice to FACEBOOK to Comply with the French Data Protection Act within Three Months, February 9, 2016, https://www.cnil.fr/en/french-data-protection-authority-publicly-issues-formal-notice-facebook-comply-french-data; Felipe Busnello and Giancarlo Frosio, WhatsApp in Brazil?, CIS Blog, December 28, 2015, https://cyberlaw.stanford.edu/blog/2015/12/whatsapp-brazil; Mark Scott, Russia Prepares to Block LinkedIn After Court Ruling, THE NEW YORK TIMES, November 10, 2016, http://www.nytimes.com/2016/11/11/technology/russia-linkedin-data-court-blocked.html (as LinkedIn does not comply with recent legal obligations in Russia that require all companies doing business in the country to store their data locally).

[143] *See* Maria Farrell, How the Rest of the World Feels About U.S. Dominance of the Internet. Short Answer: Not Great, SLATE, November 18, 2016, http://www.slate.com/articles/technology/future_tense/2016/11/the_u_s_should_stop_lecturing_about_internet_values.html.

[144] Fleisher, *supra* note 129 (emphasis added).

over any information assets belonging to their citizens. They demand their own rules to be applied to their own citizens. They want their own constitutional safeguards, checks and balances to be applied to national citizens wherever their rights are violated in the Internet.

How to cope with these concerns? These are very serious issues that will occupy international public debate for the years to come. There is no optimal solution, at least while waiting for Cyber Westphalia—or a new Internet order. For now, only global blocking governed by a nationality principle—as suggested by CNiL and other EU institutions—rather than blocking based on geo-localization, would put at rest protectionist concerns. If companies cannot cope with the laws and values of a certain jurisdiction, they always have the option of not operating there. If worldwide preoccupations are not adequately addressed, we might witness a future of information segregation and network disintegration. In the long run, harmonization—raising users' rights globally through multi-stakeholder and international consensus—will be the goal to pursue.