Articles

Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information

By Krystyna Kowalik-Bańczyk & Oreste Pollicino[*]

Abstract

Google's position in the information market has caused interesting legal developments insofar as its obligations are concerned. On various grounds, courts worldwide have begun to impose injunctions on Google that require the company to withdraw the search results—in fact, information sources—that its search engines provide. This article looks at this recent phenomenon of imposing obligations on Google to withdraw some information through the lens of judicial dialogue. In particular, we analyze the "inspiring" role of the Court of Justice of the European Union (CJEU) in its *Google Spain* judgment. This case represents a clear migration of some ideas that might be perceived as universal. Some courts outside of Europe—such as Canada—are gaining "inspiration" from the CJEU's *Google Spain* judgment in order to reinforce their own decisions. The legitimacy and techniques of this process are also discussed in this article.

[*] ***Krystyna Kowalik-Bańczyk*** is Associate Professor at the Institute of Law Studies, Polish Academy of Sciences; from September 1, 2016 a judge at the General Court of the European Union. ***Oreste Pollicino*** is Full Professor of Constitutional Law and Media Law at Bocconi University, Milan. The article is the result of a common effort: Krystyna wrote the introduction and parts B.I-III and C; Oreste wrote parts A I-II and B-IV of this text.

A. Methodological Introduction

In 2014, the Court of Justice of the European Union (hereinafter CJEU) delivered one of the most commented-on judgments known as *Google Spain*.[1] The broad outcry after this verdict was a result of the universal impact this American company[2] has, via their prominence, on everyone's access to information on the Internet.[3] Seventy-one percent of Internet searches worldwide are done through Google[4]. Not surprisingly, the case has both vocal detractors and supporters. On the one hand, there are arguments questioning the authority of national or international courts to issue worldwide orders directed at a company outside of their jurisdiction. On the other hand, these courts claim there are legitimate reasons to demand that Google withdraw some information selected and provided by its search engines.

In antitrust law, a company's size does not result in automatic suspicion.[5] In other areas of law, however, it is not as common to place special responsibility on a company due to its dominance in a particular market, especially in a situation where the company appears to be acting lawfully, at least in principle. To impose an obligation to withdraw information can appear to be an unwarranted intrusion into Google's business activities. Yet, there is a

---

[1] *See* Case C-131/12, Google Spain v. Agencia Española de Protección de Dato (May 13, 2014), http://curia/europa.eu/ [hereinafter *Google Spain]*.; *see also* Eleni Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12,* Google Spain, SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, 14 HUM. RTS. L. REV. 761 (2014); John W. Kropf, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12*, 108 AM. J. OF INT'L L. 502, 502–509 (2014); *see also* Jonathan Zittrain, *Is the EU Compelling Google to Become About.me?*, HARV. L. BLOGS (May 13, 2014), http://blogs.law.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/ (providing comments on the case); Steeve Peers, *The CJEU's Google Spain Judgment: Failing to Balance Privacy and Freedom of Expression*, EU L. ANALYSIS (May 13, 2014), http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeus-google-spain-judgment-failing.html; Paul Bernal, *Opinion: Google Privacy Ruling Could Change How We All Use the Internet*, CNN INT'L (May 14, 2014), http://edition.cnn.com/2014/05/13/business/opinion-google-privacy-bernal/index.html.

[2] Google is a publicly traded company incorporated in Delaware, USA. Its head office is located in Mountain View, California, and its Internet search services are operated in that facility. Internet users are not restricted to using the website dedicated to their particular country.

[3] On the responsibilities of search engines as user data controllers as of 2008, *cf.* OPINION 1/2008 ON DATA PROTECTION ISSUES RELATED TO SEARCH ENGINES, DATA PROTECTION WORKING PARTY (2015).

[4] *Analytics Without the Bots: Desktop Search Engine Market Share in April 2016*, NETMARKETSHARE (Apr. 2016), https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0.

[5] The dominance itself is not illegal; it is the abuse of this dominance that is questioned. S*ee* ADI AYAL, FAIRNESS IN ANTITRUST: PROTECTING THE STRONG FROM THE WEAK (2014) (providing a critical analysis of the issue). The author's point is illustrated by the pending antitrust proceeding against Google, led by the European Commission since 2010, where the European Commission is still negotiating commitments. *Cf.* Joaquín Almunia, European Commission Press Release on *Statement on the Google Investigation*, EUR. COMM'N (Feb. 5, 2014), http://europa.eu/rapid/press-release_SPEECH-14-93_en.htm.

developing sense that Google Inc., at present the biggest search engine on the Internet, has become a "Goliath,"[6] to which there is no alternative if one wants to share information on the Internet. Google's particular position in the market has prompted questions about its obligations to the public. Courts around the world, on multiple grounds, have begun to impose injunctions on the company, requiring it to withdraw search results and retract certain sources of information. The legitimacy of these injunctions is sometimes obscure and some commentators rightly claim that it might lead to a "memory hole" in some areas of information[7] and clash with the very right to information.[8]

This article looks at this recent phenomenon of imposing obligations on Google under the privileged perspective of judicial dialogue and judicial cross-fertilization. In particular, we examine the "inspiring" role, with regard to the phenomena related to the migration of judicial ideas, of the CJEU in its *Google Spain* judgment. This represents the clear migration of some ideas that might be perceived as universal. Some courts outside of Europe, such as Canada, rely on the CJEU's *Google Spain* judgment to reinforce their own decisions. Due to the potential influence of *Google Spain*, the legitimacy and techniques of this decision need to be further analyzed.[9]

Against this background, this article assumes the following theoretical framework: The interaction between interconnected and non-interconnected legal systems in the judicial body best explains and explores these issues. This new and complex field is known as "judicial dialogue."[10]

---

[6] *See* Alison Smale, *In Germany, Strong Words Over Google's Power*, N.Y. TIMES (Apr. 16, 2014), http://www.nytimes.com/2014/04/17/business/international/in-germany-strong-words-over-googles-power.html?_r=0.; Mathias Döpfner, *An Open Letter to Eric Schmidt: Why we fear Google*, FRANKFURTER ALLGEMEINEZEITUNG (Sept. 11, 2014), http://www.faz.net/aktuell/feuilleton/debatten/mathias-doepfner-s-open-letter-to-eric-schmidt-12900860.html.

[7] See Jeff Roberts, *Canadian Court Forces Google to Remove Search Results Worldwide, as Fears of "Memory Hole" Grow, GIGAOM* (July 25, 2014), https://gigaom.com/2014/07/25/canadian-court-forces-google-to-remove-search-results-worldwide-as-fears-of-memory-hole-grow/.

[8] *See* Oreste Pollicino & Marco Bassini, *Reconciling Right to be Forgotten and Freedom of Information in the Digital Age: Past and Future of Personal Data Protection in the European Union*, 2 DIRITTO PUBBLICO COMPARATOR italiano ed europeo 641 (2014); *See also* Neelie Kroes, Press Release, *Freedom of Expression is No Laughing Matter: Media Freedom in the Internet Age*, EURO. COMM'N (Sept. 2, 2014), http://europa.eu/rapid/press-release_SPEECH-14-575_en.htm.

[9] The Court makes this very clear in points 57 and 58 of the reasons for the judgment of the Supreme Court of British Columbia, Equustek Solutions Inc. v. Jack, [2014] B.C.S.C. 1063 (Can.) [hereinafter *Equustek*].

[10] *See* ORESTE POLLICINO & MARCO BASSINI, THE INTERACTION BETWEEN EUROPE'S LEGAL SYSTEMS: JUDICIAL DIALOGUE AND THE CREATION OF SUPRANATIONAL LAWS (2012); *see* Ricardo Lorenzetti, *Global Governance: Dialogue Between Courts*, 3 EUR. UNIV. INST. 1 (2010); Francis G. Jacobs, *Judicial Dialogue and the Cross-Fertilization of Legal Systems: The European Court of Justice*, 38 TEX. INT'L L.J. 547–56 (2003).

From a judiciary standpoint, it is important to analyze what precisely the courts are examining in their opinions. There are two connected issues being contested: (1) The increasing globalization of Internet law and (2) the judicial balancing of contrasting rights in the digital era. These interconnected issues may be viewed as Internet law studies which together constitute one side of the coin. The other side consists of judicial dialogue.

Seen in this format, it is necessary to elucidate two points: First, a judicial dialogue-based approach provides added and innovative value for Internet law studies (the first side of the coin). Second, within the substantive parameters of Internet law, including the protection of fundamental rights within the digital environment, the consideration of European and global judicial interaction also constitutes an advantage for judicial dialogue (the second side of the coin).

I. Internet Law Studies

When it comes to Internet law, the courts' involvement is rarely a spontaneous action and is more often a reaction to a collision—or risk of a collision—between legal systems in identifying the most suitable means to effectively protect the fundamental rights at stake.

Today, more than ever, courts' respective legal orders and privileged position enable them to identify risks of encroachment, and this reality encourages them to forge closer ties between different yet interacting systems. Given the extent of contemporary judicial globalization, the court's crucial position of influence—and their judicial dialogue—is further amplified when it comes to protecting fundamental rights in our interconnected digital-age world.

This is especially true due to two peculiarities of the Internet—one substantive and one procedural in nature. The substantive peculiarity concerns the awareness that legal reforms tend to lag behind technological advances. The burden of making up for this inevitable legislative inertia—at a national and supranational level—falls heavily on the shoulders of the courts. This article adopts the perspective, however, that the novelty of the factual and legal context created by the Internet is even more interesting and complex. Indeed, its novelty is one of the main reasons why courts increasingly seek assistance to protect the fundamental rights on the Internet to a greater extent than they do in the analogical world. Courts find such assistance in other courts of different yet interconnected legal orders. The procedural peculiarity underlying the choice to focus on interaction between the courts relates to the jurisdictional issues that the worldwide web (the "Web") brings. As we noted in the first part of this article, these jurisdictional issues have had crucial implications on fundamental rights protection and have led to an amplification of the "judicial dimension" of the field.

Bearing this in mind, Internet law has also been the object of very specific technical studies, especially by U.S. scholars who have long posed two questions: (1) whether the

Web can be subject to legal regulation and (2) which "entity" has the power to impose such regulation. In Europe, this debate has been almost monopolized by Internet and IT lawyers, who have explored the field from a very specific perspective, focusing mainly on the relationship between law and technology. In other words, the topic's peculiarities have fascinated a specialized group of Internet lawyers, but have not attracted as many scholars interested in the multilevel protection of fundamental rights from a European constitutional perspective. This is a natural consequence of the fact that the Internet represents a major innovation—perhaps first and foremost from a technical point of view. Its reach and implications, however, touch upon basic human individual and social issues.

II. Judicial Dialogue

With regard to the other side of the coin, the outflow of judicial research provides a good reason to support looking at European judiciary interaction through the substantive lens of Internet law—specifically the protection of fundamental rights in the digital environment. In recent decades scholars have focused their studies on relationships between courts, particularly in the fields of constitutional and European law. This scholarship resulted in a variety of debates concerning the relationship between the two "European courts"—the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR)—and the national courts of respective Member States. Scholars have largely focused their attention on the reasons, effects, and mode of operation of such interaction, while few cases have focused on its substantive content. Court rulings have mainly been examined not because of the added value they had in terms of enhanced protection for certain rights, but because of their importance in the relationships with other courts and, more generally, from the perspective of judicial interaction between interconnected legal systems.

Focusing on a substantive issue—in this case, the protection of right to privacy versus the freedom of speech on the Internet—provides concreteness, substance, and an unequivocal direction for future scholarship. The lack of substantive focus, along with the often overly vague and general theorization of specific features, is the Achilles' heel of the studies on judicial dialogue.

In light of the methodological framework described above, this article aims to decipher various courts' underlying reasoning for finding a link between a private party's act of placing information on a webpage and Google's obligation to restrain access to certain information that appears in the results of its search engines. To do this, we begin by briefly giving examples of court judgments that imposed such an obligation. Then, we analyze the reasons why some courts have justified the imposition of this obligation on Google's legal activities and freedom of business. Finally, we explore the mechanism of cross-fertilization—or judicial dialogue—that took place between the CJEU and the Canadian jurisdiction as an example of the migration of judicial ideas worldwide. We investigate the special features of this particular migration, focusing on the main "European judicial idea,"

which seems to have caused the migration of the idea of an individual's absolute right to digital privacy. This article concludes by providing a critical assessment of what might emerge next in this area of law.

B. The Question of Jurisdiction of Non-United States Courts over Google

By virtue of the fact that it is the biggest search engine in the world, Google Inc. has become involved in legal conundrums covering, among other things, privacy issues and intellectual property disputes. Google cases provide many opportunities for the examination of these issues. Courts rely upon the "blame Google phenomenon" to resolve some of the legal disputes taking place between parties other than Google. Two recent judgments clearly illustrate the trend and justification of shifting liability on Google.

The first example of a blame-shifting judgment is the already-mentioned CJEU case, *Google Spain*, involving the so-called "right to be forgotten,[11] and the second is the judgment of the Supreme Court of British Columbia, *Equustek Solutions Inc. v. Jack* of June 13, 2014,[12] followed by the order of the Canadian Court of Appeal for British Columbia, *Equustek v. Google* of July 23, 2014.[13] The article will explain how the CJEU's judgment in *Google Spain* influenced the Supreme Court of British Columbia in two ways. First, it invoked the CJEU's judgment in order to explain its "global" or universal jurisdiction over Google. Second, the Canadian Court defined the obligations of Google in a way similar to the CJEU arguments.[14] Thus, Google's "unhappy precedent,"[15] set by the CJEU, is likely to be used on a broader scale and not only within the European Union (EU).

In international law, in order to claim "jurisdiction to enforce,"[16] courts might refer to different connecting factors giving rise to such jurisdiction: The principle of territoriality,[17] the principle of nationality, the principle of the passive jurisdiction (the "effects" doctrine)

---

[11] Interestingly, the ECtHR has not accepted this right, *see cf.* Węgrzynowski and Smolczewski v. Poland, App. No 33846/07 (Oct. 16, 2013), http://hudoc.echr.coe.int/.

[12] *See generally Equustek*, B.C. S.C. 1063.

[13] Equustek Solutions Inc. v. Google Inc., [2014] B.C.C.A. 295 (Can.) [hereinafter *Equustek Solutions*].

[14] *See Equustek*, B.C.S.C. 1063 at para. 57–58; *See also Equustek Solutions*, B.C.C.A. 295 at para. 5.

[15] *See Equustek Solutions*, B.C.C.A. 295 at para. 8.

[16] This is distinct from "jurisdiction to prescribe," which allows for creating laws for a certain territory. *Cf.* Opinion of Advocate General Darmon, Joined Cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85, C-125/85, C-126/85, C-127/85, C-128/85, C-129/85, Ahlström v Comm'n, 1994 E.C.R. I-00099, para. 28.

[17] *See* Dieter G.E Lange & John Byron Sandage, *The Wood Pulp Decision and Its Implications for the Scope of EC Competition Law*, 26 COMMON MKT. L. REV. 137, 139 (1989).

or, more rarely, universal jurisdiction.[18] Most legal texts use the territoriality principle, including EU Directive 95/46,[19] which the CJEU applied in the *Google Spain* case. The courts must justify their jurisdiction and find the applicable law. Under EU law, we often observe a solution that Joanne Scott calls "territorial extension," which is a judicial technique that justifies the application of EU law, while any "extraterritorial application" of jurisdiction remains rare.[20]

I. Google Spain

The *Google Spain* case concerned a situation where Google Inc. and its Spanish subsidiary—Google Spain (both referred to hereinafter as Google/Spain)—provided search results on Mario Costeja González. Those search results directed any Internet user searching the term "Mario Costeja González" to the source web pages of a Spanish newspaper from 1998. Mr. González contested the accessibility of those pages, stating that the information they contained was no longer relevant and should no longer be displayed.[21] The case reached the CJEU as a preliminary reference from *Audiencia Nacional* (the National High Court of Spain) lodged during administrative proceedings between Google Spain SL and Google Inc (hereinafter the "Google/Spain") and the *Agencia Española de Protección de Datos* (hereinafter the "Agencia") with Mr. González.

The proceedings concerned the application of the Data Protection Directive[22] to an Internet search engine that Google/Spain, as a service provider, operated. The *Agencia* issued a decision ordering Google/Spain to withdraw the data from its index and to restrict further access to the information. Google/Spain appealed this decision and the *Audiencia Nacional* decided to refer several questions to the CJEU. These questions concerned the territorial scope of application for EU data protection rules,[23] the legal position of an

[18] *See* MALCOLM N. SHAW, PRAWO MIĘDZYNARODOWE (INTERNATIONAL LAW) 351–60 (Książka i Wiedza ed., 2000).

[19] *See* LOKKE MOEREL, THE LONG ARM OF EU DATA PROTECTION LAW: DOES THE DATA PROTECTION DIRECTIVE APPLY TO PROCESSING OF PERSONAL DATA OF EU CITIZENS BY WEBSITES WORLDWIDE? 28 (2010).

[20] *See* Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law*, 62 AM. J. COMP. L. 87 (2014).

[21] The pages contained two announcements in *La Vanguardia* concerning a real estate auction connected with attachment proceedings prompted by social security debts. Mr. González was mentioned as the owner of the property. At a later date, an electronic version of the newspaper was made available online by its publisher—there is no citation as it has been "forgotten."

[22] Directive 95/46 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) will be replaced by the Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119). It shall apply from May 25, 2018.

[23] Directive 95/46 of the European Parliament and of the Council of 24 October 1995, 1995 O.J. (L 281) has been the object of CJEU interpretations on various occasions, however, never on the issues of Internet search engines.

internet search engine service provider, and the right to be forgotten, including whether data subjects can request that some or all search results concerning them no longer be accessible through the search engine. As the CJEU described in its judgment, Google Inc. is a California firm with subsidiaries (so-called "data centers") in some Member States of the EU, including, for example, Ireland, Belgium and Finland.

According to Google, no processing of personal data by its search engine was taking place in Spain. Google argued that the office of Google/Spain was merely an in-country commercial representative of Google Inc. and only processed personal data relating to Spanish advertising and Spanish customers. Google denied performing any operations on the host servers of the source web pages or collecting information by means of the cookies of non-registered users by its search engines. Thus, the dispute was between a California firm acting together with its Spanish commercial representative against a Spanish national who requested that both companies remove any possibility of finding particular data by use of the search engine. The data itself was not illegal; it was just Mr. González who argued that despite the legality of the information, it should have been removed from the Internet because it damaged his reputation. The CJEU found against Google/Spain on the grounds of the EU's personal data protection rules and the exercise of right to be erased.

To better understand the context in which the *Google Spain* case took place, it is worthwhile to examine various legal instruments concerning the trans-border transfer of personal data. When Directive 95/46 was adopted, it was strongly influenced by the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention") of the Council of Europe, even partly mirroring its solutions. It was only the additional protocol to Convention No. 108 that regulated the question of data flows from a party to the Convention (the forty-five Council of Europe Member States and Uruguay).[24] This Protocol omits, as does the Convention itself, questions linked with the choice of law and conflicts of laws.[25] The Convention only states, in the newly revised version of Article 3, that a State Party to the Convention has jurisdiction if the data subject

---

Cf., Case C-101/01, Lindqvist, 2003 E.C.R. I-12971; Case C-195/06, ÖsterreichischerRundfunk, 2007 E.C.R. I-08817; Case C-73/07, SatakunnanMarkkinapörssi and Satamedia, 2008 E.C.R. I-09831; Joined Cases C-92/09, C-93/09, Volker und Markus Schecke & Eifert, 2010 E.C.R. I-11063. The question of Internet search engines did appear in cases on intellectual property rights and the jurisdiction of courts. *See* Joined Cases C-236/08, C-237/08, C238/08, Google France and Google, 2010 E.C.R. I-02417; Case C-558/08, Portakabin Ltd. and Portakabin BV v. Primakabin BV, 2010 E.C.R. I-06963; Case C-324/09, L'Oréal SA & Others v. eBay International AG & Others, 2011 E.C.R. I-06011; Case C-323/09, Interflora Inc. & Interflora British Unit v. Marks & Spencer Plc. and Flowers Direct Online Ltd., 2011 E.C.R. I-08625; Case C-523/10, Wintersteiger AG v. Products 4U Sondermaschinenbau GmbH (Apr. 19, 2012), http://curia.europa.eu/.

[24] LEE ANDREW BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 38 (2014).

[25] *Id.* at 39.

is covered by its jurisdiction.[26] There is, however, no clear criteria for determination of that jurisdiction.[27]

In contrast, the OECD guidelines on privacy protection and trans-border data flows provide a rule indicating that the data controller is responsible for the trans-border flow of personal data.[28] Paragraph 16 of the OECD Guidelines states that "a data controller remains accountable for personal data under its control without regard to the location of the data."[29] Departing from the model of Convention No. 108, Directive 95/45 was "the first and only international data privacy instrument to tackle directly the vexed issue of which national law is applicable to a given case of data processing," as observed by Lee Bygrave.[30] The basic rule for the choice of law contained in Article 4(1)(a) of the Directive[31] requires that one verify the establishment or place of business of a data controller.[32] Surprisingly, the CJEU in *Google Spain* did not refer to any comparative analysis of the texts that might have assisted in the construction of the EU norms.[33]

In order to properly comment on *Google Spain*, one must cite Christopher Kuner who postulates that the present method of identifying law and jurisdiction relies primarily on the location of data. He refers to the "origin of data" as a "modern application of the doctrine of personality," comparable to nationality in earlier times.[34] In 2013, he suggested that European data should be protected wherever it is processed, which, in a way, pre-announced the *Google Spain* solution. In contrast, in *Google Spain*, the CJEU used a "trigger" that Joanne Scott calls "subsidiary jurisdiction," which holds that foreign companies fall under the jurisdiction of EU legislation if they own subsidiaries that hold the

---

[26] *Id.* at 40.

[27] *Id.*

[28] *O.E.C.D. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited June 7, 2013).

[29] This expression replaced the previous "equivalency with domestic legislation," as noted in BYGRAVE, *supra* note 24, at 48.

[30] *Id.* at 63.

[31] *See supra* note 3.

[32] *See* MOEREL, *supra* note 19, at 29; LOKKE MOEREL, BACK TO BASICS: WHEN DOES EU DATA PROTECTION LAW APPLY? 92–110 (2011).

[33] Such a comparative and international approach is suggested by Graine de Búrca in cases where the CJEU acts as a constitutional adjudicator. *Cf.* Grainne De Búrca, *After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?* 5 (N.Y.U., Working Paper No. 13-51, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2319175&rec=1&srcabs=2276433&alg=1&pos=3.

[34] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 123 (2013).

nationality of an EU Member State.[35] It was this latter assumption, and not Kuner's "origin of data" idea, that the CJEU used as a basis for finding jurisdiction, and to apply EU law—in *Google Spain*.[36]

While *Google Spain* analyzed the scope of Directive 95/46's application, CJEU Advocate General Jääskinen proposed considering the question of the territorial applicability of privacy "from the perspective of the business model of internet search engine service providers."[37] To do this, one must examine keyword advertising as a source of income and as the main reason for the provision of the free information location tool (or search engine). The entity that is in charge of keyword advertising is usually present on the national advertising market. For this reason, Google has established subsidiaries in EU Member States and provided national web domains for these subsidiaries, such as "google.es" for Google Spain. Thus, a controller[38] of data is present in the territory of a Member State in accordance with Article 4(a) of Directive 95/46.

Directive 95/46 imposes on Member States an obligation to protect personal data even if "the processing of data is carried out by a person established in a third country."[39] The CJEU stated that "processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State" [40] in cases where the operator of a search engine sets up, in a Member State, "a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State."[41] In *Google Spain*, the CJEU did not claim any global jurisdiction over Google; it only justified the jurisdiction of the Spanish judicial bodies over those Google actions linked with Spanish territory.

---

[35] Joanne Scott, *The New EU "Extraterritoriality"*, 51 COMMON MKT. L. REV. 1343, 1352 (2014).

[36] *See Google Spain*, Case C-131/12 at para. 54–61.

[37] See *Google* Spain, Case C-131/12 at para. 64.

[38] A "controller" is defined in Directive 95/46 of the European Parliament and Council of Europe of 12 October 1995, art. 2(d), 1995 O.J. (L 281) as "the natural or legal person . . . which alone or jointly with others determines the purposes and means of the processing of personal data." The CJEU found that an Internet search engine is a controller within the meaning of that provision. *Cf. Google Spain*, Case C-131/12 at para. 33.

[39] Directive 95/46 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) preamble, para. 20.

[40] *See Google Spain*, Case C-131/12 at para. 60.

[41] *See Google Spain*, Case C-131/12 at para 45.

Apart from what constitutes an "establishment" for the purposes of jurisdiction, another important notion is "data transfer." The CJEU defined "data transfer" in *Lindqvist*,[42] where it stated that website publishing does not constitute a data transfer for the purposes of Article 25 of Directive 95/46.[43] What *Lindqvist* avoided—making Directive 95/46 a text of universal application due to a broad definition of data transfer—became an issue that arose twelve years later with *Google Spain*. Due to the CJEU's judgment in *Google Spain*, the Directive is now interpreted as covering all situations in which the data of European subjects are processed. This controversial solution allows for the EU Directive to apply to data controllers established outside of the European Union—what Bygrave calls "the extraterritorial effect."[44]

II. Equustek Solutions Inc. v. Jack

Google Spain served as a clear formulation of the obligations imposed on Google in the second case analyzed in this article, which comes from outside the EU. In *Equustek Solutions Inc. v. Jack*, the Supreme Court of British Columbia issued an injunction with extra-territorial effects against Google, a non-party. The circumstances of the case were as follows: The plaintiff, Equustek Solutions Inc., a manufacturer of networking devices, claimed that the defendants, Morgan Jack and Datalink Technologies Gateways Inc., while acting as a distributor for the plaintiff's products, conspired with one of the plaintiff's former engineering employees to design and manufacture a competing product. The defendants were also hiding, for several years, the plaintiff's name and logo on products and distributing the plaintiff's products as their own. Later, while manufacturing the competing product, the defendants were exclusively advertising the plaintiff's products on their websites. When they obtained orders, however, the defendants delivered their own competing product.[45] The plaintiff commenced an action against the defendants in April 2011. The defendants failed to comply with various court orders. Instead, they began to operate as a virtual company only, carrying out their business through a complex and ever-expanding network of websites which advertised and sold their product. These websites

---

[42] BYGRAVE, *supra* note 24, at 191.

[43] *See Lindqvist*, Case C-101/01 at para. 69:

> If article 25 of Directive 95/46 were interpreted to mean that there is a transfer [of data] to third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where thee are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the Internet.

[44] BYGRAVE, supra note 24, at 200–01 (listing other countries that possess rules modeled on DPD article 4, such as Austrialia's federal Privacy Act, US Children's Online Privacy Protection Act 1998, Malaysian Personal Data Protection Act of 2010).

[45] This is a tactic called "bait and switch."

were subject to numerous court orders prohibiting the defendants from carrying out said business through any website. Following those orders, Google voluntarily complied with Equustek Solutions' request to remove specific webpages or uniform resource locations (URL) from its "google.ca" search results. Google removed 345 URLs in total.[46] But Google was unwilling to block an entire category of URLs—called "mother sites"—from its search results worldwide. On June 13, 2014, the plaintiff obtained an interim injunction restraining Google Inc. from indexing or referencing specific websites, identified in the schedule to the plaintiff's notice of application, in search results performed on its search engines. The Supreme Court of British Columbia forced Google to delete search results visible to the whole world, not just those found in "google.ca," but also those found on "google.com." Google challenged the order's enforcement, but the Court of Appeal of British Columbia ruled on July 23, 2014 that this decision would not create "irreparable harm."[47] Thus, the Canadian courts ordered Google to censor its search results worldwide, not just on its Canadian search engine.

In its response to the enforced injunction, Google claimed that the Canadian Courts do not have jurisdiction over Google Inc., or even Google Canada, because neither of the websites were present in British Columbia.[48] Esquustek Solutions's order was, according to Google, a "worldwide order" that could not be enforced and would constitute an unwarranted intrusion into Google's lawful business activities as a search engine. The Supreme Court of British Columbia did not accept Google's position.[49] The Supreme Court of British Columbia referred to a text by Kevin Meehan which states that the Internet is an "environment of geographic anonymity" and that the "principles of international jurisdiction, particularly territoriality, are poorly suited for this sort of environment."[50] The Canadian Court concluded that Google's Internet search websites are not passive information sites for several reasons: (1) Google anticipates the request and offers a menu of suggested potential search queries; (2) Google collects a wide range of information as a user

---

[46] *See Equustek*, 2014 B.C.S.C. 1063, at para. 72–73 (providing an explanation why this process was unsatisfactory). The Court referred to the decision of the *Tribunal de Grande Instance GI Paris* of November 6, 2013 in *Max Mosely v. Google France SARL and Google Inc*. This French criminal proceeding considered the following circumstances: The newspaper "News of the World" videotaped Mosely while he was engaging in sexual activity with several partners. The newspaper published the images and made others available on its website. The court found the newspaper guilty and ordered the newspaper to cease publishing the images, but the images remained widely available by searching through Google Images. Mosely asked Google to stop indexing those pictures with reference to specific URLs. Google honored all of Mosely's requests, but the images continued to be indexed and searchable through new URLs.

[47] *See generally Equustek Solutions*, B.C.C.A. 295.

[48] *See Equustek Solutions*, B.C.C.A. 295 at para. 9.

[49] *See Equustek Solutions*, B.C. C.A. 295 at para. 9, 16.

[50] Kevin A. Meehan, *The Continuing Conundrum of International Internet Jurisdiction*, 31 B.C. INT'L & COMP. L. REV. 345, 349 (2008). *See also Equustek*, B.C.S.C. 1063 at para. 37.

searches; and, most importantly, (3) Google sells advertising to clients in the territory concerned—in this case British Columbia clients. By entering into an advertising contract with the defendants, Google's Internet search websites were no longer passive information sites.[51]

Google had previously questioned this reasoning, stating that its advertising services are completely separate from its search services. The Canadian court found that, for two reasons, no such separation can be asserted: First, Google's business model consisted of contextual advertising. Ads were thus linked either to the subject matter of the search or to the history of the person searching. To develop this reasoning, the Canadian court referred to *Google Spain*, where Google raised the same arguments concerning the CJEU's jurisdiction.[52] Both courts agreed that the two parts of Google's business—advertising and search functions—were inextricably linked. As a second argument for rejecting Google's contentions, the Supreme Court of British Columbia ruled that the fact that one of the two interlinked activities has a weaker relation with a given territory does not affect the Court's territorial competence. The Canadian Court concluded that if Google decides to do business on a global scale, it must, as a consequence, accept that any court of any state in the world would have global jurisdiction over Google's search services.[53]

The Canadian court borrowed the same reasoning from *Google Spain* that once the "establishment" of a company is found a court may claim global jurisdiction. One could legitimately question whether a Canadian court has territorial competence over a worldwide internet search provider and whether a Californian court is not better placed to adjudicate. The Canadian court found that the claim against Google "may be considered to be a claim for an injunction ordering a party to refrain from doing something in relation to movable property in British Columbia."[54] The court ruled that even though one of the two interlinked activities had a weaker relation with a given territory, it did not affect the court's territorial competence.[55] According to the Canadian Court, Google's Internet search websites were not passive information sites. Google claimed that such global injunctions would affect information accessible to Internet users around the world and that individuals, rather than the specific content, should have been targeted in this action. Google opposed the injunction because it was granted against a non-party conducting a legitimate business independent of any wrongdoing by the defendants.

---

[51] *See Equustek*, B.C.S.C. 1063 at para. 48–50.

[52] *Google Spain*, Case C-131/12 at para 56.

[53] *Equustek*, B.C.S.C. 1063 at para. 64 ("I will address here Google's submission that this analysis would give every state in the world jurisdiction over Google's search services. That may be so. But if so, it flows as a natural consequence of Google doing business on a global scale, not from a flaw in the territorial competence analysis.").

[54] *Equustek Solutions*, B.C.C.A. 295 at para 7.

[55] *See Equustek Solutions*, B.C.C.A. 295 at para. 3.

In both judgments, the courts made an effort to find a link with the national territory in order to justify the application of European law—or in the Canadian case, national law—to define Google's worldwide obligations. In all areas of EU law which extend beyond EU territory—for example, competition, financial, and privacy law—Joanne Scott stated that "the line between territorial jurisdiction and extraterritorial jurisdiction becomes difficult to draw" as it is unclear whether "the triggers that the EU is relying on should be understood as territorial or not."[56] In fact, in the following analysis of both cases, the territorial connection, used to established jurisdiction of the adjudicating courts, took into account Google's active advertising practices, which are directly connected to its search services.

III. The Underlying Reasons for Claiming Jurisdiction to Impose Obligations on Google

The paradox of *Google Spain* exists in the fact that the CJEU required Google to exercise the "right to be forgotten" with respect to entirely legal information concerning a private party. There was no breach of law involved, nor was any tort committed by one party against another, which Google was obliged to "correct" by eliminating the information. In the Canadian case, a court proceeding between two competing manufacturers and distributers since 2012, the court found various torts committed by the defendants. The order against Google was aimed at fulfilling previous judgments. Although each case presents a different set of circumstances, both judgments align in their expectation that Google should resolve legal disputes that, in actuality, involve parties other than Google. Unfortunately, the justification for this rationale is rather scarce, particularly in the Canadian case. Whereas *Google Spain* might be explained in the broader context of privacy standards that may at least profess to be universal, the Canadian case is purely an individual solution to an individual dispute. The Canadian case involves Google in the forum of tort law.

The main reason for posing an obligation on Google in *Google Spain* seems to be a desire to protect human rights, particularly the right to privacy, contained in the Charter of Fundamental Rights of the EU (the Charter) and in Directive 95/46. One can question whether a private actor such as Google is obliged to protect human rights, including privacy interests, but at present it is rather common for most jurisdictions to expect such responsibility within a national context.[57] Nonetheless, in the international level—for example, the problem of applying the ECtHR to this scenario—there would be no "state

[56] Joanne Scott, *supra* note 35, at 1343–44.

[57] *See generally* M. Forde, *Non-Governmental Interferences with Human Rights*, 56 BRIT. Y.B. INT'L L. 253 (1985) (providing information of the evolution of this concept). Another question would be to the attribution of State responsibility to the actions of Google, but that issue is outside the scope of this paper.

action," so the Convention would not apply.[58] Usually, "international human rights guarantees do not impose legal obligations directly on the shoulders of individuals" unless directly provided by treaty.[59] It seems, however, that the Charter is a text which imposes a horizontal obligation on individuals[60]—Google in this case—to respect the privacy of EU data holders. The judgment reflects a European perspective on privacy interests, but not necessarily a global one.[61]

Thus, it is enough to have a branch or subsidiary that orients its activity towards a Member State to substantiate the jurisdiction of EU courts and to apply EU law—both the Directive and the Charter of Fundamental Rights. In *Google Spain*, the CJEU stated that the ease by which information can be replicated on different sites beyond the initial one requires the publisher to do more than erase that information from its website.[62] Relatively speaking, because the access to information is much easier with the list of results displayed by a search engine, such a tool can play a decisive role in the dissemination of information that might infringe on a person's fundamental rights.[63] That might be the case even if the publication itself is lawful.[64] The CJEU has thus required the operator of a search engine to remove from search results links that interfere with the data subject's fundamental rights if that person requests the removal. Such a right may override both "the economic interest of the operator of the search engine" and "the interest of the general public in finding that information upon a search relating to the data subject's name."[65]

Despite the differing nature of the interests involved, the Canadian court relied on *Google Spain*'s opinion. If one considers the previous judgments of the CJEU which concerned Google in cases linked with international property infringements (IPR), however, this inspiration is not confirmed. To the contrary, in the case of *Google France SARL and Google Inc. v. Louis Vuitton Malletier,* decided March 23, 2010, the CJEU stated that an intermediary service provider was not responsible for the content generated by advertisers

---

[58] *See* Campbell and Cosans v. UK, App. No. 7511/76 (Feb. 25, 1982), http://hudoc.echr.coe.int/.

[59] Forde, *supra* note 57, at 279.

[60] Nicolas Cariat, *L'invocation de la Charte des droits Fondamentaux de l'Union Européenne dans les Litiges Horizontaux : état des lieux après l'arrêt Association de médiation sociale*, 2 CAHIERS DE DROIT EUROPEEN 305, 305–336 (2014).

[61] *See generally* L.G. Loucaides, *Personality and Privacy under the European Convention on Human Rights*, 61 BRIT. Y.B. INT'L L. 175 (1990) (providing more on privacy in the broader sense).

[62] *Google Spain*, Case C-131/12 at para 84.

[63] *Id.* at para 87.

[64] *Id.* at para 88.

[65] *Id.* at para 97.

and users.[66] This conclusion was later confirmed by *L'Oreal v. eBay.*[67] The EU's e-commerce directive does not hold Google responsible because it is an intermediary service provider; therefore, the Canadian Court's analysis greatly differs from recent decisions. Taking into account the CJEU's previous IPR or unfair competition rulings, *Google Spain* should not be read to extend jurisdictional reach to cases concerning torts not committed by innocent third parties.

In light of the comparative analysis of the Canadian and EU decisions, our main assumption remains: Judicial opinions foster theoretical discussions that result in investigation and constitutional balancing between contrasting rights in the Internet era. Legal concepts and constitutional ideas seem to migrate—along with the globalized spill-over effect of reducing geographical distances—through the judicial interaction between judges who are part of different, and at times disconnected, legal orders.

IV. The Mechanism of Judicial Dialogue

Three features create the basis of this "judicial" migration which is at the heart of the Canadian court's ruling: (1) the transfiguration, (2) the direction, and (3) the topics of migration. The first important element is the "transfiguration" of judicial dialogue when the field moves from atoms to bits.[68] To elucidate, it is uncontroversial that in the analog environment binding effects adhere to judicial interaction only when the latter is framed in a multilevel vertical dimension. In other words, only within quasi-federal legal orders, in which there is an interconnection among autonomous but coordinated legal systems, can one envision a form of judicial dialogue which could go beyond a voluntary, non-binding, mutual inspiration. This is the case in legal systems such as EU Member States, the European Union, and the ECtHR. In contrast, all the other forms of judicial interaction between autonomous and non-interconnected legal orders, such as in the Canadian case, are generally framed in a horizontal dimension characterized by voluntary, and therefore non-binding, judicial borrowing.

If this is the classic expression of judicial dialogue in the world of atoms, then a sort of "transfiguration" emerges when the judicial interaction takes place in a digital context, as

---

[66] Joined cases C-236/08 & C-238/08, Google France SARL and Google Inc. v. Louis Vuitton Malletier SA, 2010 E.C.R. I-2417, para. 107, http://curia.europa.eu/juris/document/document.jsf?text=&docid=83961&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=747648.

[67] Case C-324/09, L'Oréal v. eBay Int'l, 2011 ECR I-6011.

[68] NICHOLAS NEGROPONTE, BEING DIGITAL 5 (1995). According to Negroponte's analysis the best way to appreciate the merits and consequences of being digital is to reflect on the difference between bits and atoms. More precisely he focuses on the economic, institutional and (indirectly) legal implications of the shift from materiality (world of atoms) to immateriality (world of bits).

explained in the cases examined in this article. Looking at the Canadian court's reasoning, one gets the impression that the court considered itself almost bound by European case law it so extensively quoted.

The Supreme Court of British Columbia's opinion exemplified the above-mentioned judicial approach in which the Canadian judges ruled on two of Google's arguments based on previous judgments of European and U.S. courts. First, Google made reference to *Yahoo v. LICRA*,[69] litigated in the United States, to support its claim that the Canadian court should not have made an order that could affect searches worldwide. Google argued that the order might cause it to contravene a law in another jurisdiction. The Canadian court took this reliance in *Yahoo* very seriously, admitting that

> *Yahoo* provides a cautionary note. As with *Mareva* injunctions, courts must be cognizant of potentially compelling a non-party to take action in a foreign jurisdiction that would breach the law in that jurisdiction. That concern can be addressed in appropriate cases, as it is for *Mareva* injunctions, by inserting a *Baltic* type proviso, which would excuse the non-party from compliance with the order if to do so would breach local laws.[70]

[69] *See* Yahoo! Inc. v. La Ligue Contre Le Racism et L'Antisemitisme, 169 F. Supp. 2d 1181, 1172 (N.D. Cal. 2001) [hereinafter Yahoo!]. In 2000, two French anti-racism groups filed suit in France against Yahoo!, alleging that Yahoo! had violated a French law prohibiting the display of Nazi paraphernalia by permitting users of its internet auction services to display and sell such artifacts. The plaintiffs demanded that Yahoo's French subsidiary, "Yahoo.fr," remove all hyperlinks containing the offending content to the parent website, "Yahoo.com." Like Google, Yahoo! argued that the French Court lacked jurisdiction over the matter because its servers were located in the United States. The French Court held that it could properly assert jurisdiction because the damage was suffered in France and required Yahoo! to "take all necessary measures" to "dissuade and render impossible" all access via "yahoo.com" by internet users in France to the Yahoo! Internet auction service displaying Nazi artifacts, as well as to block Internet users in France from accessing other online Nazi material. Yahoo! claimed that implementing the order would violate its First Amendment right to freedom of expression and that the judgment could not be enforced in the United States. The French Court did not accept that submission. Hence Yahoo! initiated a suit in California against the French plaintiffs and obtained a declaratory judgment that the French order was constitutionally unenforceable in the United States, because it was contrary to the First Amendment. Addressing the issue of international comity, the Court reasoned that United States courts will generally recognize and enforce foreign judgments but could not do so on the facts of the case before it because enforcement of the French orders would violate Yahoo!'s constitutional rights to free speech. *See also Yahoo!,* 169 F Supp 2d at 1192–93. This decision was ultimately reversed on different grounds: *See also* Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 379 F.3d 1120 (9th Cir. 2004) and Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F.3d 1199 (9th Cir. 2006).

[70] *Equustek*, B.C.S.C. 1063 at para. 143.

After delineating this line of reasoning, the British Columbia Supreme Court demonstrated even more self-perception of the binding nature of *Yahoo* by emphatically distinguishing what was at stake before it from what was at stake in *Yahoo*. More precisely, the Court added that

> Google is before this Court and does not suggest that an order requiring it to block the defendants' websites would offend California law, or indeed the law of any state or country from which a search could be conducted. Google acknowledges that most countries will likely recognize intellectual property rights and view the selling of pirated products as a legal wrong.[71]

Second, Google argued that a worldwide removal order would be a disproportionate remedy. In support of this argument, it relied on the *Max Mosely*[72] decision of the Tribunal de Grande Instance (Paris). More specifically, Google argued that in *Max Mosely* the court fully accepted Google's argument that removing images should be restricted to searches that could be conducted from within France. The Canadian court based its answer to the second argument on a different judicial precedent—one based in European case law; the court's response shows even more clearly the perceived quasi-binding nature of court decisions, even those belonging to different and not interconnected legal orders.[73] These are decisions which, in the world of atoms, would be considered mere guidance and would never have been subjected to the formal process of being distinguishing as was done in the Canadian Court ruling. To counter Google's argument, the Canadian court formally distinguished the case in front of it. It was as though the court was operating in a common law system, forced to separate its decision from that of another court of the same or higher legal order.

Given these considerations, one may derive the impression that a global common law on internet matters, with a privileged channel of expression in the form of judicial dialogue, is emerging. Even if framed horizontally, it is clearly acquiring some vertical features more typical of judicial interaction that occurs among courts belonging to a federal or quasi-federal legal system. In this respect, the alteration of the classic notion of judicial dialogue seems like an irreversible process.

---

[71] *See Equustek*, B.C. S.C. 1063 at para. 144.

[72] BYGRAVE, supra note 24, at 191.

[73] We refer here to kinds of interaction which belong to the horizontal dimension of the judicial conversation and which generally are deprived of any binding character.

The second element of judicial migration is its direction. Case law analysis reveals that, at least until now, the migration is almost exclusively unidirectional. European judges "export" European ideas outside Europe. Put differently, European courts' rulings, which are extensively quoted in an attempt to increase the legitimacy and persuasiveness of their own rulings, inspire and influence non-European Union judges. Any reverse treatment appears to be largely outside of the judicial agenda at the moment. The European courts seem more inclined "to teach" rather than "to learn" when discussing the protection, *erga omnes* (towards everyone), of European constitutional values, even beyond the reaches of Europe. In other words, the European judicial dialogue remains European-value-based even when globalized. It would be strange, and even paradoxical, if it took the opposite path.

The third element connected to judicial migration is related to the subjects of the migration. More precisely: Which main European ideas are migrating across the Ocean?

The CJEU's reasoning in *Google Spain*[74] possibly asserts that the main idea consists in the CJEU's attempt to adapt the right to privacy to the characteristics of the digital world. Warren and Brandeis depicted this looking at the world of atoms.[75]

Some doubt remains as to whether the CJEU may have taken too seriously the issue relating to the definition and protection of this new right. As a result, it may have neglected the consequences that are likely to derive from this new approach, which was most probably brought about by the scandal surrounding the NSA case. Two negative consequences should be carefully considered:

The first consequence of this new approach is the possible underestimating of the implications of offering such an extreme degree of protection afforded to personal data vis-à-vis the protection of other constitutional values—for example, other fundamental rights. Above all, this concerns freedom of expression. Furthermore, there is a risk that such an extreme approach may result in an excess of "Europeanization" in the Internet's regulation.

With regard to the first risk, the freedom of expression receives less protection in the digital world. As noted above, the absence of any express reference to Article 11 of the

---

[74] The same outcome emerges from analysis of the case of *Digital Ireland,* in which the CJEU declared Directive 2006/24 of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) on the retention of data (for example, data retention) to be invalid because of its inconsistency with some provisions of the European Charter of Fundamental Rights. *See* Joined Cases C-293/12, C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources (Apr. 8, 2014), http://curia.europa.eu/.

[75] *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

Charter in *Google Spain* is only one of the signals confirming that the balance struck by the CJEU seems to be skewed in favor of the right to digital privacy. A consequence of this overbalancing is that it results in a degree of protection of the freedom of expression on the Internet that is lower than the standard of protection the Court grants it in non-digital freedom of expression cases. Such a trend is also visible in the ECtHR which, although it uses different arguments, seems to reach the same conclusions as the CJEU,[76] downgrading the protection of freedom of expression when it is exercised on the Internet.[77]

Turning back to *Google Spain*, we observed that Articles 7 and 8 of the Charter did not provide legal parameters. The Court seems to have assumed that these provisions have horizontal effects as well.

One of the most relevant statements in this respect is paragraph 96 of *Google Spain*. Here, the Court of Justice questioned whether a person has a right to request that information relating to him or her no longer link to the search results generated by an Internet search of his or her name. The only way to reach an affirmative answer to this question was to recognize that Article 8 of the Charter has horizontal effects. This would be true assuming that the information at stake was true, impartial, and—as the Advocate General noted—was deprived of a specific legal foundation in Directive 95/46.

This is a crucial point. The provision of the fundamental rights enshrined in the Charter, with direct and horizontal effects, seems to be the only viable option to remove the obstacles to private actors who seek to protect their fundamental Internet rights. The European Court of Justice, in its 2013 annual report, stressed the importance of such application.[78]

The *Aklagaren* case clearly explains the court's approach. The judges held that

> European Union law precludes a judicial practice which makes the obligation for a national court to disapply any provision contrary to a fundamental right guaranteed by the Charter conditional upon that infringement being clear from the text of the Charter or the case-law relating to it, since it withholds from the

[76] *See* Oreste Pollicino, *Internet Nella Giurisprudenza Delle Corti Europee: Prove Di Dialogo?,* FORUM DI QUADERNI COSTITUZIONALI (Dec. 31, 2013), http://www.forumcostituzionale.it/wordpress/images/stories/pdf/documenti_forum/paper/0454_pollicino.pdf (providing more detail).

[77] Delfi v. Estonia, App. No. 64569/09 (Oct. 10, 2013), http://hudoc.echr.coe.int/.

[78] *See* VASSILIOS SKOURIS, REPORT OF THE COURT OF JUSTICE: CHANGES AND ACTIVITY 2 (2013).

> national court the power to assess fully, with, as the case may be, the cooperation of the Court of Justice, whether that provision is compatible with the Charter.[79]

With respect to the second risk, there are at least two signals that reveal possible detrimental consequences, especially in terms of excessive "Europeanization" of the Internet's regulation. One example of this Europeanization is the Court of Justice's adoption of an extreme data-based or data-oriented approach.

The first signal is the rapidly growing stronger inclination to apply EU law on data protection every time a case concerns European citizens, especially if the citizen is an individual resident in the EU. First, courts apply EU law regardless of the circumstances surrounding the processing of personal data. If the effects were not felt in Europe, the analysis takes into account the place where the controller is established and not solely the place where the relevant equipment is located. Second, courts apply EU law regardless of where the process servers are located.

The extensive interpretation given to the "context of the activities" of an establishment brings the CJEU to the same conclusion that it would most likely have reached by applying Article 3, Paragraph 2 of the Proposal of Regulation on Data Protection.[80] In fact, the Court has taken an expansive interpretation of this expression to mean that a controller is not necessarily the same subject that materially operates the processing of personal data. According to Article 3, Paragraph 2 of the Proposal of Regulation, even though the controller is established outside of the European Union, EU law is nevertheless applicable if the processing activities that involve personal data imply providing or targeting products or services to individuals residing in the EU.

By using these provisions, the Court of Justice has sped up the creation of new rules, immediately applicable, which renders future (and oftentimes delayed) reforms useless. Those who are unfamiliar with the CJEU's typical role of playmaker in adopting European integration processes may be unfamiliar with this phenomenon.

The second signal that brings to light the risk described above deals with the problem of the physical place of retention of personal data. This is a part of the alarming trend toward

---

[79] Case C-617/10, Åklagaren v Hans Åkerberg Fransson, para. 48 (Feb. 26, 2013), http://curia.europa.eu/.

[80] *Proposal for a Regulation of the European Parliament and of the Council Concerning the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, EUR. COMM'N (Jan. 5, 2012), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en.

excessive "Europeanization" of the Internet by the European judges. This approach can be seen in how the Court of Justice invalidated the data retention directive—moving its attention from the problem of applicable law to the physical infrastructure—and specified that because the "directive does not require the data in question to be retained within the European Union . . . it cannot be held that the control, explicitly required by Article 8, paragraph 3 of the Charter, by an independent authority of compliance with the requirements of protection and security . . . is fully ensured."[81] In this case, the Court of Justice refers to Article 8, paragraph 3 of the Charter to justify the requirement that personal data of individuals residing in Europe, which are processed in order to prevent attacks against national security, are stored within the territory of the Member States.

The problems of determining the applicable law and the place of data storage are two pieces of the same project of the European courts aimed at making European law, and European territory, an eventual fortress in the protection of individual personal data. It is a fortress that, even if otherwise considered impregnable, might lack the necessary flexibility to ensure the actual extraterritorial application of EU law, which is needed to adequately protect the right to digital privacy. This is the most critical point of the process of judicial Europeanization of the Internet. The Internet's transnational nature makes it incompatible with attempts to regionalize protection, despite the fact that such attempts are inspired by the aim to increase the degree of such protection.

The contrast between the territorial limits of enforcement jurisdiction and the global nature of the service—against which decisions are enforced—risks a "race to the bottom" in the protection of the rights at issue and of a lack of enforcement mechanisms of such protection. Indeed, it is a further expression of the conflict between local law and global law that characterizes judicial globalization and of which the law of the Internet constitutes a privileged field of investigation.

C. Conclusions

Google Spain raised an outcry in both academic and legal practice circles. Some scholars perceive that the CJEU is overtaking the ECtHR's leading position as the developer of fundamental rights in Europe. Others have proclaimed that the way the CJEU ordered Google to behave was an act of judicial activism. At the same time, the *Google Spain* judgment also brought about an unprecedented reaction in different judicial *fora*. Just one month after the seminal judgment, the Canadian courts followed the CJEU's reasoning in order to justify disregarding the principle of territoriality when they claimed jurisdiction over Google. For the Canadian Court, selling advertising services in their country created a sufficient nexus over which the Court could assert jurisdiction. It is important to note that the courts did not require Google to monitor the sites' content provided by the defendants

[81] *Digital Rights Ireland*, C-293/12, C-594/12 at para 68.

in the analyzed cases. Rather, the courts required Google to remove the websites from its searches, in the same manner as it would require the removal of hate speech or child pornography websites.

The judgments presented demonstrate that the principle of territoriality diminishes in importance vis-à-vis technological progress.[82] Technology allows for transfers of information without regard to national borders. Courts are beginning to confirm this reality. If one sticks to the principle of territoriality, even while information can move literally around the globe, the enforcement of any judicial decision can be questioned. Google, as a global company, clearly takes the risk of global jurisdiction over its business activity. The strong European influence on this process, as revealed in this article, is a clear example of the "migration" of CJEU ideas.

[82] This is not a new phenomenon. It was already noted at the time of drafting of 1980 OECD Guidelines on privacy. *See* Michael Kirby, *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, 1 INT'L DATA PRIVACY L. 6, 7 (2011).