GLOBAL IDENTITY MANAGEMENT FOR INDIVIDUALS? THE RIGHT TO BE FORGOTTEN AND ISSUES OF EXTRATERRITORIALITY

Petra Lea Láncos[1]

DOI: 10.24989/ocg.v331.8

Abstract
The Google Spain ruling of the Court of Justice of the European Union has received much attention (and criticism) both in Europe and the other side of the Atlantic. In this paper I present the decision, focusing on it novel elements and the issues of extraterritoriality. I analyse the problems of extraterritoriality as a function of jurisdiction relying on the presence or absence of links to the EU through the location of establishment, equipment or the target of business activity. Next, I discuss the arguments promoting and rejecting the global application of Rtbf by search engine operators. Finally, I consider extraterritoriality as a practical problem, the solutions offered by scholarship and national courts, as well as their effect on corporations.

1. Introduction

The internet has radically altered the concept of memory – and with it, the public perception of individuals. While the human brain recalls images, sounds etc. in an arbitrary and incomplete way, servers around the world store uploaded data accurately and comprehensively. Yet while the identity of an individual may be reconstructed with the use of data available online, these are all but a snapshot of the diverse life of the person concerned, willing to change and denounce earlier habits or beliefs. Besides relying on the normal workings of human memory, the law has long employed gag orders, anonymity rules, restrictions on access to archives, etc. to promote criminal rehabilitation or to protect privacy. These instruments are rendered more or less ineffective, however, with the perpetual memory of our increasingly digital world.

In its ruling C-131/12 Google v AEPD and González the Court of Justice of the European Union established the right to be forgotten in European Union law, a concept also enshrined in the new General Data Protection Regulation (GDPR). The right to be forgotten seems to be an important legal tool complementing more traditional instruments ensuring accuracy, up-to-dateness, lawfulness and the protection of data. While the right to be forgotten fits seamlessly with European privacy standards, service providers outside the EU are reluctant to adhere to it. In particular, they assert that any request invoking the right to be forgotten beyond European top-level domains is an effort at exerting extraterritorial jurisdiction. Meanwhile, search engine operators resist undertaking new legal, economic and technical obligations.

In the proposed paper I briefly describe the online context of privacy and personality rights violations. Next, I analyse the problems of extraterritoriality as a function of jurisdiction relying on

[1] Researcher, Deutsches Forschungsinstitut für öffentliche Verwaltung, Freiherr-vom-Stein-Str. 2, 67346 Speyer, Germany. Associate Professor, Pázmány Péter Catholic University, Faculty of Law and Political Sciences, Szentkirályi utca 28, 1088 Budapest, Hungary. lancos.petra.lea@jak.ppke.hu.

the presence or absence of links to the EU through the location of establishment and business activity. In particular, I focus on the relevant ruling of the Court of Justice of the European Union (CJEU), revealing the open questions of jurisdiction and the problems of implementing the ruling. Indeed, unresolved issues concerning the extent of search engine operators' obligations and the preliminary reference submitted by the Conseil d'État render this question highly topical. I examine extraterritoriality as a practical problem and consider various solutions proposed in scholarly literature. Finally, I draw some tentative conclusions and raise the issue whether or not the CJEU actually vindicates the authority of global identity management to EU law.

2. Forget-Me-Nots of the Online World

In the analog world, technological advances progressively increased both the speed of spreading news and the accessibility of content on an ever larger scale. News spread by word of mouth, then through newspapers, and eventually, radio and television. Meanwhile, information became a commodity, persons of interest became celebrities and readers and viewers became the consumers in a market where in contrast with backstreet gossip, participants offering and seeking information no longer know each other, with an entire industry built on satisfying the insatiable demand for news. To curb pushy media workers and intrusive paparazzi scraping for crumbs of new information and to restrain editorial rooms keen on landing best-selling headlines, national legislation and regional fundamental rights mechanisms were developed seeking to afford effective protection to private life, personality rights and personal data. Jurisprudence on the protection of public figures and the right to information also evolved.

The digital revolution of the past decades constitutes a new landmark in the evolution of information technology by yet again elevating the spreading and accessibility of information to a higher level. The creation of the world wide web and the availability of multimedia devices was a game changer for the media market, affecting both its structure and actors. Content travels rapidly within our online global village reaching millions, with Web 2.0 websites turning erstwhile consumers into content providers. Media service providers and the advertising sector suffer drastic structural changes, dissipating the traditional *gate keeping* functions of editorial rooms. Information is released unfiltered, spreading unbridled beyond borders and jurisdictions. Anonymity, editing techniques, the speed of spreading information and the multitude of unverified sources lead to the phenomena of 'revenge porn', 'fake news', 'fake porn', etc. calling the credibility of information available online into question. Meanwhile, the „internet doesn't forget":[2] years after publication, information may be easily found and spread online (see [2], p. 84). Every second, a vast amount of data is uploaded to hosting sites, while the content is searchable and may be shared in almost real time. In this context, violations of privacy and personality rights are further exacerbated through the unimpeded spreading of injurious information online (see [4], p. 3).

The shifting technological landscape elicited different solutions from national legislators seeking to meet challenges emerging online and to strike a balance between various fundamental rights, such as the freedom of expression and freedom of information on the one hand, and the respect for

[2] As Marks summarizes: „Since the Google algorithm is not chronologically based, it will be hard for [those concerned] to "escape" their pasts because of the Internet's "inability to forget." (…) If a case that is over a decade old can be revisited in such detail so as to be considered "newsworthy" again and tarnish the image of those who had been able to distance themselves from the events of their past, where is this line drawn? At what point does the Internet's memory begin to intrude upon the protection of one's sense of self? How can one reconcile the American dream of being able to be whoever you want when people can no longer escape their past or change preconceived notions of who they are or what they stand for?" (see [8], p. 42-43).

private life and the protection of personal data on the other (see [18], p. 245; [13], p. 223). At the same time, in the cross-border context of online offences standard questions of private international law may arise regarding the applicable law, the forum having jurisdiction, the territorial scope of the decision taken and even the party liable for implementing the decision. While legislators have been faced with the difficulty of regulating and restricting online activity and arriving at effective solutions for protecting individual rights, this does not mean that legislators could waive their regulatory tasks or the enforcement of privacy and personality rights.

In 2014 the Court of Justice of the European Union breathed new life into Union data protection rules by declaring the right to be forgotten in its *Google Spain* ruling. Against the backdrop of a borderless internet the ruling and the questions surrounding its implementation shed fresh light on extraterritoriality, i.e. the exercise of jurisdiction over activities occurring outside its borders (see [16], p. 227). In the following, I analyse the *Google Spain* ruling to understand the factors the CJEU took into account in order to bring Google Inc. under the *ratione personae* of EU data protection law.

3. Main Findings of the *Google Spain* case

In the instant case, Mario Costeja Gonzales filed a complaint with the Spanish Data Protection Authority in 2009 against La Vanguardia Ediciones SL, Google Spain and Google Inc. Following a *vanity search*, Mr. Costeja Gonzales discovered that the website of the daily publication La Vanguardia featured decade old information on his erstwhile social security debts and auctioning off of his property. Mr. Costeja Gonzales did not deny the veracity of this information, yet he insisted that he had settled his debt years ago and requested that the Spanish Data Protection Authority oblige La Vanguardia to erase or alter the information relating to him and to take action against Google Spain or Google Inc. to remove or conceal the personal data relating to him so that the data no longer appeared in the search results and in the links to La Vanguardia, since these are no longer relevant.[3] The Data Protection Authority upheld the complaint against Google Spain and Google Inc., who in turned challenged the decision before the national court. In the instant case, several question were referred to the CJEU requesting a preliminary ruling.

In its Google Spain ruling[4] the Court of Justice of the European Union declared that under certain conditions, search engine operators are obliged to remove links from the list of results displayed following a search made on the basis of a person's name upon request of the data subject. This right of the data subject enforceable against search engine operators has come to be known as the right to be forgotten. Legislation has since caught up to CJEU case law and the new General Data Protection Regulation of the EU applicable as of 25 May 2018 expressly refers to the right to be forgotten in its Article 17.[5]

The right to be forgotten is not without antecedents (see [11], p. 11; [17], p. 134). indeed, it is the online equivalent of the right to blocking foreseen under the Data Protection Directive.[6] The

[3] Court of Justice of the European Union: Press Release No. 70/14 (Luxembourg, 13 May 2014).
[4] C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD).
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), see further recitals (65) and (66).
[6] 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 OJ *L 281 , 23/11/1995. 0031 – 0050.*

Directive regulates blocking under the title "The data subject's right of access to data" in Article 12 para b) as follows: „Member States shall guarantee every data subject the right to obtain from the controller: (…) as appropriate the rectification, erasure or *blocking* of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data."[7] Hence, exercising the right to be forgotten actually means enforcing the right to blocking in an online environment, 'in particular' for reasons of the incomplete or inaccurate nature of the data involved. The latter expression is of great significance, since the applicant in the *Google Spain* ruling did not deny the completeness or accuracy of the data. However, since cases for exercising the right to blocking in Article 12 paragraph b) of the Directive were preceded by the phrase *in particular*, the CJEU arrived at the conclusion that the list in question was not exhaustive. Accordingly, the Court of Justice of the European Union concluded that the right to blocking may be enforced under other circumstances as well. These include situations where the data concerned „are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary."[8] With this, the CJEU did not necessarily extend, but more precisely defined the scope of cases where the right to be forgotten may be exercised.

The most important contribution of the *Google Spain* ruling is therefore that the Court of Justice of the European Union clarified: EU data protection rules, such as the right to blocking must be implemented in the online context as well (*delisting*). As far as the online context is concerned, the CJEU emphasized that the simple searchability of data makes access to and dissemination of information appreciably easier, which "is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page."[9] This is due to the fact that while sites included in the search results generally published the information concerning the data subject lawfully, collecting such content and making the readily accessible to internet users may magnify the harm caused. Thus, the CJEU separated the individual responsibility of the editor of the website and that of the search engine operator and opened the door to claims made against search engine operators for violation of the data subject's right to privacy. In light of the *Google Spain* ruling of the CJEU, the sole obligor of the right to be forgotten is therefore the search engine operator.

An important finding of the ruling is that the privacy rights of the data subject under Articles 7 and 8 of the Charter of Fundamental Rights „override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having (...) access to the information in question" (see [11], p. 10).[10] The Court of Justice of the European Union clarified that legal recourse is available to the data subjects irrespective of whether the inclusion of the information in the search results causes prejudice to the data subject.[11] This means that delisting requests made by the data subjects do not have to substantiate the occurrence of any specific harm. As a corollary, the search engine operator may only exceptionally deny delisting requests. In case the data concerned is inaccurate, incorrect or no longer relevant, internet users' freedom of information must give way to the data subject's right to privacy (see [19], p. 1122) which, in turn must be enforced by the search engine operator upon request of the data subject concerned. Hence, as a rule, it is the data subject who may decide whether or not information related to him should be readily accessible, albeit only in hindsight. Exceptions, i.e. the denial of a delisting request shall be

[7] Italics by me.
[8] Ruling, para 92.
[9] Ruling, para 87.
[10] Ruling, operative part, para 4.
[11] Ibid.

based on the role played by the data subject in public life and the preponderant interest of the general public in gaining access to the information in question (see [18], p. 250). With this, the CJEU laid down the test to be applied when assessing cases involving the right to be forgotten.

The question, however, arises: on what basis did the Court of Justice of the European Union include Google Inc., a company established in the United States of America, under the scope of European Union law and the jurisdiction of national courts? In the following, I discuss the findings of the CJEU in respect of jurisdiction as well as the relevant question raised in scholarly literature analysing issues of extraterritoriality in the *Google Spain* ruling.

4. Establishing Jurisdiction in *Google Spain*

In its ruling rendered in the *Google Spain* case, the Court of Justice of the European Union declared that search engine operators must be considered 'controllers'[12] within the meaning of the Data Protection Directive, while their activity must be classified as 'processing',[13] since they collect, retrieve, record, organize, store, disclose and make available data in the form of lists of search results.[14] Consequently, activities of search engine operators fall under the scope *ratione materiae* of the Data Protection Directive (see [15], p. 658-659).

The issue of extraterritoriality was raised in relation to the scope *ratione personae* of EU data protection law, the central question being whether a company established in the United States of America, such as Google Inc. may be bound by obligations set forth under Union law. According to the International Law Commission, extraterritoriality is "an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law".[15] As Kuner emphasizes, in light of its definition, whether we are speaking of extraterritorial jurisdiction depends on "whether the jurisdictional grounds apply to conduct that takes place outside the State that has enacted it or to parties in another country" (see [7], p. 7). The solution chosen by the CJEU to establish jurisdiction actually calls into question whether we can label it extraterritorial, for although it invokes jurisdiction over conduct outside the EU, it attributes this conduct to a party within its jurisdiction.

Namely, according to the CJEU the link to Union law is established by the fact that data processing is carried out *in the context of the activities* of the Spanish subsidiary of Google Inc., that is the company Google Spain.[16] While the subsidiary Google Spain itself carried out no processing and its activities were limited to the sale of advertising space, the CJEU was satisfied, that establishment of Google Spain in the territory of the EU and the processing activities of Google Inc. create the link necessary to establish jurisdiction. Namely, the Data Protection Directive „does not require the processing of personal data (...) to be carried out 'by' the establishment concerned itself, but only

[12] According to Article 2 para d) of Directive 95/46/EC 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.
[13] Article 2 para b) of Directive 95/46/EC.
[14] Ruling, para 28.
[15] International Law Commission (ILC), "Report on the Work of its Fifty-Eighth Session" (1 May-9 June and 3 July-11 August 2006) UN Doc A/61/10, Annex E, para. 2.
[16] Ruling, paragraphs 52-55.

that it be carried out 'in the context of the activities' of the establishment".[17] In other words, „the activities of the operator of the search engine and those of its establishment situated in the Member State are *inextricably linked* since the activities relating to the advertising space constitute the means of rendering the search engine at issue profitable and that engine is, at the same time, the means enabling those activities to be performed."[18] The inextricable link between the different activities of Google Inc. and Google Spain is further evidenced by the fact that „the very display of [search] results is accompanied, on the same page, by the display of advertising linked to the search terms, [making it] clear that the processing of personal data in question is *carried out in the context* of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory".[19]

An interesting feature of the instant case in Google Spain was therefore that the activities falling under the scope ratione materiae and the territorial scope of EU law were different, including the legal persons carrying these activities, namely the controller on the one hand, and the EU undertaking on the other. However, in order to guarantee effective protection to the data subjects, the Court of Justice of the European Union attempted to piece together jurisdictional links from the facts of the case under the concept of the inextricable *link* of the companies and the activities concerned. As the CJEU elaborated, „the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope."[20] In Scott's assessment, „the EU engages in the practice of *territorial extension* to prompt or provoke different types of legal or behavioural change. (...) Here, the EU is playing the role of a norm catalyst, with the EU measure in question serving to alter the regulatory baseline against which third countries asses the costs and benefits of taking action to address the problem concerned" (see [14], p. 106-108).

Accordingly, the Court of Justice of the European Union seems to rely on the territorial principle when establishing jurisdiction over Google Inc. based on its inextricable link with Google Spain (see [4], p. 8). However, alluding to the principle of effectiveness, the contours of an effects-based jurisdiction may also be discerned. Indeed, according to some scholars Article 4 of the Data Protection Directive establishing jurisdiction is perhaps the most contradictory, misunderstood and enigmatic provision of the Directive (see [3], p. 228). In the course of negotiations on the text of the Directive the concept of processing in the territory of a Member State was gradually broadened, leaning towards a solution based on territorial jurisdiction. At the same time, the Union legislator was aware of the danger that companies may seek to locate their servers in states with more lax data protection regimes, thereby posing the threat of evading jurisdiction based on the territorial principle (escamotage) (see [11], p. 31-32). Therefore, the final text of the Directive related to jurisdiction includes the following wording: „each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State". This broad concept of territorial jurisdiction is coupled with an equally broad understanding of establishment, as evidenced by recital (19) of the Directive's preamble which states that irrespective of the legal form of the undertaking, „establishment on the territory of a Member State implies the effective and real exercise of activity through stale arrangements" (see [15], p. 661). Scott describes this legal construct as follows: „these natural or legal persons may

[17] Ruling, paragraph 52.
[18] Ruling, paragraph 56.
[19] Ruling, paragraph 57.
[20] Ruling, paragraph 54.

either be regarded as being present within the EU or as engaging in EU conduct on the basis that they are offering the services concerned" (see [14], p. 92).

5. The Extent of Delisting Obligations

5.1. Right to be Forgotten: Regional or Global Reach?

According to one point of criticism outlined in scholarly literature, the Google Spain ruling will remain ineffective, since search engine operators will continue to provide unrestricted access to the data concerned 'outside the EU'. In consequence, the protection granted under the right to be forgotten will be rendered illusory (see [18], p. 245). All of this begs the question: what is the extent of the search engine operator's obligation under the right to be forgotten, that is, on which search pages does the search engine operator have to delist the results as requested by the data subject?

As far as the scope of the delisting obligation is concerned, it is worth recalling that in its ruling the Court of Justice of the European Union did not declare that Google Inc. must only delist results covered by the request on national versions of the Google search page. Conversely, it also failed to indicate that the ruling must be implemented globally, on all search pages, including all third country national versions and that with the global web extension .com. This question was left open by the CJEU and was also left unresolved by the GDPR.

The Article 29 Working Party, a consultative body established under the Data Protection Directive, proposed that the delisting be carried out on all relevant pages, including those with the web extension .com. In professional literature this was then interpreted in a way that the Working Party does not suggest global delisting, but merely the enforcement of the right to be forgotten on Member State national versions of the search page and the .com web extension. Following the ruling Google Inc. established an Advisory Council to give guidance on how to fulfil its obligations stemming from the right to be forgotten.[21] The Advisory Council consists of ten members, professionals in the field of data protection, digitalization and information rights, seeking to advise Google on balancing the rights and interests of data subjects and the public at large (see [11], p. 17). The Advisory Council pointed out that 95 percent of all search queries in the Member States are carried out on the national versions of the search pages and not the google.com. That is, internet users do not exploit the opportunities provided by the global search engine (see [17], p. 125).Therefore, the Advisory Council concludes that „in the current state of affairs and technology", removing links from the search results of European versions will provide adequate protection to data subjects (see [11], p. 17). Yet in the current state of affairs it is easily conceivable that the remaining 5 percent of search queries are carried out on the global search page of Google for the very reason that the information sought was not to be found on the national version of the search page, effectively circumventing the restrictions imposed to enforce the right to be forgotten. This would be in stark contrast with the principle of effective legal protection. At this point, the question arises: in case Google Inc., a company established outside the European Union can be included under the scope of Union law, why should the consequences of the enforcement of the right to be forgotten be restricted to the EU national versions of Google?

[21] https://archive.google.com/advisorycouncil/

5.2. CNIL and Global Identity Management

Indeed, this was the position underlying the decision of the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL). One year after the Google Spain ruling and „in the interest of effective legal protection" the CNIL obliged Google in its decision to implement the delisting of results on all of its search pages. According to the CNIL the „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."[22] Namely, according to the CNIL the Google Spain ruling of the CJEU must be interpreted in a way that delisting requests upheld by the search engine operator must be implemented across all web extensions.[23] Should delisting be limited to only certain extensions, it could easily be circumvented, leading to a hollowing out of the right to be forgotten and the application of different rights to individuals depending on queries of the internet user.[24] The CNIL also pointed out that even a comprehensive delisting affecting all search pages would not amount to a negation of the information rights of the public at large, nor to content censorship, since the content will remain accessible, albeit searchable with different terms and freedom of information will remain under the supervision of CNIL and the national courts.[25]

Google appealed to the Conseil d'État against the decision of the CNIL, arguing that were we to allow the application of one region's law to the entire world, „internet would only be as free as the world's least free place" (see [9]).[26] The extraterritorial application of French (or rather, Union) law is a slippery slope in Google's view, which would be to the detriment of French internet users' information rights and opportunities in the long run. It is important to note that similar concerns were also voiced by academics in scholarly literature – Svantesson goes so far as to envision situations were oppressive dictatorships exploit the opportunity of global delisting to block critical content (see [17], p. 14). Finally, Post raises the question whether the right to be forgotten may lawfully restrict the freedom of expression (see [12], p. 706).

It is important to note that the operation of efficient search engines is a common interest, contributing to asserting individuals' freedom of information. Indeed, search engines may be considered an important element of the communications market, promoting a wide array of fundamental rights directly linked to individuals' information rights. Search engines facilitate access to wide range of political, religious, business, scientific and artistic information underpinning fundamental rights such as freedom thought, political rights, freedom of enterprise, academic and artistic freedom, etc. All this, however, does not mean that search engine businesses would have a legitimate expectation of freedom from regulation: there are legitimate grounds for restricting such activities, including privacy rights of the data subjects. The legislator may thus create the framework for balancing freedom of expression, the interests of the public at large to access information and the individuals' right to privacy and to 'curate their identity' (see [5], p. 1). Regulating search engines' activities indirectly affects the public's right to information and individuals' freedom of expression rendering their assertion less efficient by making restricting easy access to lawfully published data. Therefore, regulatory intervention should not be unduly restrictive. This implies a requirement of proportionality towards the legislator, which may potentially be met should EU decision-makers codify the test devised by the Court of Justice of the

[22] https://www.cnil.fr/fr/node/15814
[23] https://www.cnil.fr/fr/node/15815
[24] https://www.cnil.fr/fr/node/15814
[25] https://www.cnil.fr/fr/node/15814
[26] Peter Fleischer, the data protection advisor's blog post is no longer accessible.

European Union for assessing delisting requests. Legislation should set forth the criteria for screening abusive requests, relying on a delimitation between public figures and information of genuine interest for the public at large, and all other information related to data subjects. Finally, judicial remedy must be available to guarantee an adequate balancing of information and privacy rights, where restrictions are justified and proportionate.

5.3. Conseil d´État paves the way towards legal certainty?

The Conseil d'État proceeding in the case was of the view that it required the clarification of various points of the applicable law and on 21 August 2017 referred several questions to the Court of Justice of the European Union requesting a preliminary ruling. Based on the questions referred, the Conseil d'État is primarily concerned with the extent of Google's delisting obligations under EU law.[27]

With its first two question the Conseil d'État essentially asks whether blocking provisions of the Data Protection Directive[28] prescribe global delisting on all search pages of the search engine operator or only the national version of the Member State where the requesting data subject resides, or all EU national versions, respectively? The third question referred implies a technical solution to prevent the circumvention of blocking: must the right to be forgotten be understood as the obligation of the search engine operator to disable access to the relevant search results by imposing geo-blocking in the Member State where the data subject resides or all EU Member States, respectively (see [1], p. 15)?

This line of inquiry seems to rely on an effects-based approach to jurisdiction which could be an adequate means to assuage extraterritoriality concerns (see [1], p. 12-13). According to the effects-based approach to jurisdiction, any and all activities liable to cause harm in the European Union shall fall under the scope of Union law, or in the present case, under the scope of European data protection law (see [11], p. 26-27; [14], p. 93]. The French Conseil d'État is likely to have been inspired by the *UEJF and LICRA vs Yahoo!* decision, where Yahoo! was sued in France for hosting a site auctioning off Nazi memorabilia. Without directly referring to geographical filtering, the Tribunal de Grande Instance de Paris obliged Yahoo! to take all technically feasible measures to make the site inaccessible in France, stressing at the same time that for the implementation of the decision, web extension-based delisting shall not suffice.[29]

6. Alternative Solutions and Outlook

Those criticizing the right to be forgotten point out that the diverse requirements set forth under the different legal systems impose serious administrative and financial burdens on search engine operators offering services on a global scale. However, in light of the possible privacy and personality rights violations caused by search engine operators, the regulation of such activities is justified. No market operator is entitled to a lack of regulation. Indeed, it is worth mentioning that the provision of other, offline services is also subject to legislative requirements, therefore, legal rules that the service provider must adhere to are a normal corollary of business operations – in this respect, search engine providers are not put at a disadvantage. On the contrary, Tassis and Peristaki

[27] Preliminary reference of the Conseil d'État submitted on 21 August 2017 – Google Inc. v Commission nationale de l'informatique et des libertés (CNIL) (C-507/17) OJ C 347, 16.10.2017, 22–23.
[28] Article 12 para b) and Article 14 para a) of Directive 95/46/EC.
[29] Rg: 00/05308 UEJF and LICRA v Yahoo!

emphasize that the fact that Union law prescribes uniform requirements under the General Data Protection Regulation can much rather be seen as a benefit, since undertakings no longer have to adapt to data protection rules differing from one Member State to the other. As such, the GDPR in fact reduces administrative burdens of undertakings by unifying the data protection law applicable in the Member States (see [18], p. 251). The sheer scale of the European communications market and its elaborate rules on data privacy may even prompt other jurisdictions to copy or converge towards its standards, creating efficiencies also for search engine operators.

Moreover, fears that Google should wind up its subsidiaries established in the European Union have no merit either, since both the effective provision of the Data Protection Directive (Article 4 read together with recital 19) and the provisions of the GDPR entering into force in 2018 (Article 3 read together with recital 22) provide, that irrespective of legal form or the seat of the undertaking, Union data protection law shall be applicable to all processing of the controller where the effective and real exercise of activities through stable arrangements in the Union are fulfilled. Of course, in practice it is difficult to envisage the enforcement of Union law against entities with no subsidiaries established, or servers located in the territory of the Member States.

These difficulties prompted several scholars to propose the regulation of the world wide web as a cross-border phenomenon in an international treaty, where signatory states could jointly regulate the use of the web as well as violations committed online (see [6]; [10]). However, as Ryngaert points out, the feasibility of such an international agreement is more than questionable, given the diversity of regulatory solutions and the balance struck between the fundamental rights of the data subject and the public at large (see [13], p. 223).

By contrast, the Conseil d'État offers the Court of Justice of the European Union an effective and much more feasible solution on a silver platter which could effectively protect privacy and personality rights. Through the application of geo-blocking with effect to the territory of the Member States, the EU could shake accusations of extraterritoriality and global identity management, implementing a technical solution that has been tested and proven worldwide. Geo-blocking would mean that third state and .com web extensions would be spared of implementing delisting requests, while content covered by the delisting request could not be searched from the territory of the Member States by recourse to non-EU search pages. The diverse balance of information rights achieved in other states would remain unaffected, while the effective protection of data subjects in the Union would be guaranteed.

Some criticize the solution referring to the fact that this way, Europeans will know less about themselves and their affairs, than anyone else in the world. However, it is worth pointing out that the test devised by the Court of Justice of the European Union guarantees that only those information be forgotten, the knowledge of which does not breach the rights and interests of the public at large. Thus, timely information of genuine interest to the public, information on public figures and public affairs continue to remain accessible.[30]

Critique is further aimed at the fact that geo-blocking does not provide absolute protection and with the help of certain technical solutions, such blocks may be circumvented. While technically no perfect means exists, this is the solution that from a legal point of view best implements the CJEU's

[30] Cf. Article 29 WP: Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles" C-131/12, 14/EN WP 225 (2014.11.26.), 2.

ruling, employing a combination of delisting on EU web extensions and geo-blocking for all other search pages. What may give rise to concern is that geo-blocking can be a means for concealing information from the population and may be used to violate information rights and to manipulate public opinion. Such potential for abuse calls for the devising an elaborate legal background for the use, supervision and technical means of geo-blocking to ensure that restricting access to information complies with constitutional standards. Principles and legal criteria governing the use of geo-blocking in general and in specific cases in particular must be set forth under EU law, including the framework for national controls on the use of geo-blocking. This entails further legislative obligations on both the supranational and the national level to operationalize this new instrument enabling the enforcement of data privacy.

Meanwhile, thanks to the Conseil d'État's request for a preliminary ruling we will soon know more about the extent of search engine operators' obligation under the right to be forgotten and whether the CJEU vindicates the authority to global identity management.

7. References

[1] VAN ALSENOY, B., KOEKKOEK, M., Internet and Jurisdiction after Google Spain: The Extra-territorial Reach of the EU's "Right to be Forgotten", in: Leuven Centre for Global Governance Studies WP. Vol. 152 (2015).

[2] BUCHMANN, J. (ed.), Internet Privacy. Options for Adequate Realization. Acatech study (May 2013).

[3] BYGRAVE, L., Data Privacy Law: An International Perspective. Oxford University Press, Oxford 2014.

[4] FOMPEROSA RIVERO, A., Right to be Forgotten n the European Court of Justice Google Spain Case: The Right Balance of Privacy Right, Procedure, and Extraterritoriality, in: Stanford-Vienna European Union Law WP. Vol. 19 (2017).

[5] GULOTTA, R.− HAAKON, F.−MANKOFF, J., Curation, Provocation, and Digital Identity: Risks and Motivations for Sharing Provocative Images Online, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2012.

[6] DE HERT, P.−PAPAKONSTANTINOU, V., Why the UN should be the world's lead privacy agency (28.04.2016.) https://iapp.org/news/a/why-the-un-should-be-the-worlds-lead-privacy-agency/

[7] KUNER, C., Extraterritoriality and International Data Transfers in EU Data Protection Law. Legal Studies Research Paper Series. No. 49 (2015).

[8] MARKS, D., The Internet Doesn't Forget: Redefining Privacy through an American Right to be Forgotten, in: UCLA Entertainment Law Review. Vol. 23 (2016).

[9] NAUGHTON, J., In the battle of free speech not it's France v Google. The Guardian (09.08.2015.).

[10] MOELLER, C., Respective Roles: Towards an International Treaty for Internet Freedom? http://www.global.asc.upenn.edu/respective-roles-towards-an-international-treaty-for-internet-freedom/

[11] PEROTTI, E., The European Ruling on the Right to Be Forgotten and Its Extra EU Implementation. WAN-IFRA (14.12.2015.) https://ssrn.com/abstract=2703325

[12] POST, R. C., A szólásszabadság amerikai hagyományának magyarázata. Wolters Kluwer, Budapest. 2017.

[13] RYNGAERT, C., Symposium issue on extraterritoriality and EU data protection, in: International Data Privacy Law. Vol. 5 (2015).

[14] SCOTT, J., Extraterritoriality and Territorial Extension in EU Law, in: The American Journal of Comparative Law. Vol. 62 (2014).

[15] STUTE, D. J., Privacy Almighty? The CJEU's Judgment in Google Spain SL v. AEPD, in: Michigan Journal of International Law. Vol. 36 (2015).

[16] SVANTESSON, D. J. B., Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, in: International Data Privacy Law. Vol. 5 (2015).

[17] SVANTESSON, D. J. B., Limitless borderless forgetfulness? Limiting the geographical reach of the ‘right to be forgotten’, in: Oslo Law Review. Vol. 2 (2015).

[18] TASSIS, S.− PERISTERAKI, M., The Extraterritorial Scope of the „Right to be Forgotten“ and how this Affects Obligations of Search Engine Operators Located Outside the EU, in: European Networks Law & Regulation Quarterly. Vol. 3 (2014).

[19] TUTT, A., The revisability principle, in: Hastings Law Journal. Vol. 66 (2005).