Is the right to be forgotten a universal, regional, or 'glocal' right?

Yann Padova*

Key Points

- The 'right to be forgotten' (RTBF), introduced by the Court of Justice of the European Union (CJEU) in its *Google Spain* judgment on 13 May 2014 is being examined again before the Court through 11 preliminary questions submitted by the French administrative supreme court (*Conseil d'Etat*)
- The 11 questions directly stem from the uncertainty that the CJEU's ruling implementation triggered and may have considerable and international consequences, far outside Europe, depending on the Court's answers
- On the substance, these questions may be grouped into two categories. The first category is related to the consequences of categorizing search engines as controllers with respect to what the Directive's Articles 8 and 9 prohibit them from doing, collecting and processing '*sensitive data and data involving an offense*'
- The second category of questions concerns the territorial scope of the RTBF, resulting from the dispute between Google and the French Data Protection Authority (the 'CNIL'), which fined the search engine €100,000. According to the questions submitted by the *Conseil d'Etat*, the CJEU has three possible options
- These two categories of preliminary questions are highly related. The choices made in one category are likely to amplify, or limit, the effects of the choices made in the other category
- The prohibition for search engines to process sensitive data added to a 'universal' territorial scope could have severe and structural consequences on how the web operates and could lower Internet users' accessibility to content on the Internet that is not originally regulated by European law

Introduction: the right to be forgotten entailed several legal uncertainties at inception

The 'right to be forgotten' (RTBF),[1] or more precisely the 'right to suppression'[2] continues its judicial saga as it is being examined by the very same Court that created it, following the submission of 11 preliminary questions[3] by the French Council of State before the Court of Justice of the European Union (CJEU).[4]

Created by the CJEU in its *Google Spain* judgment on 13 May 2014,[5] the right to be deindexed has been seen as 'triply audacious'[6] with regard to its legal implications. First, it includes in the territorial scope of Directive 95/46[7] the search engine activity performed by Google Inc. from the USA. To this end, the Court first established that, although it had only a technical role in the processing of the search engine's data, Google Inc.'s Spanish subsidiary had a business of selling advertising spaces intended for the Spanish market in order to make the service offered by Google Inc. profitable.

* Yann Padova, is a lawyer with Baker & McKenzie Paris. He is the former Secretary General of the French data protection authority (the "CNIL" - 2006/2012). Email: yann.padova@orange.fr

1 Otherwise, strictly speaking, the right to be deindexed. The three expressions will be used here, along with 'the right to be forgotten'.

2 C Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines' (2015), LSE Law, Society and Economy Working Papers 3/2015 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496060>, last revised 29 November 2015, 7.

3 These 11 preliminary questions are submitted to the French Council of State in two separate series: the first series Council of State, Mme C, M. F, M. H, M. D, no 391000, 393769, 399999, 401258 (henceforth, ''Series 1'), which includes eight questions, is dated 24 February 2017, the second series Council of State, 19 July 2017, Google Inc., no 399922 (henceforth, 'Series 2'), includes three questions dedicated exclusively to the territorial scope of the right to be forgotten.

4 Hereinafter, the 'CJEU' or the 'Court'.

5 Case C-131/12 *Google Inc. Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales* ECLI:EU:C:2014:317 (hereinafter, the '*Google Spain* judgment').

6 G Odinet and S Roussel, 'Renvoi préjudiciel, le dialogue des juges décomplexé' [Prejudicial referral, the uninhibited dialogue of judges], AJDA. 2017, 742.

7 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (hereinafter, the 'Directive').

The Court inferred from this that the personal data processing implemented by Google Inc. was 'carried out in the context of the activities'[8] of its Spanish establishment[9] and, hence, that European regulations applied. This is undeniably quite a striking decision, the potential extraterritorial legal effects of which were not demarcated by the Court.[10] Such legal effects have been the subject of lively discussions, and even controversies, which this article intends to go over in detail.

The second reason the *Google Spain* judgment is seen as audacious is because it applied the substantive legal notion of data controller to search engines. It should be recalled that the controller processing personal data is the entity that determines the purposes and means. Here again, this decision, which has far-reaching consequences, was strongly debated. Indeed, the Advocate General in his Opinion on the *Google Spain* judgment considered that 'An internet search engine service provider is not a "controller" of personal data on third-party source web pages'[11] because:

> The internet search engine service provider merely supplying an information location tool does not exercise control over personal data included on third-party web pages. The service provider is not 'aware' of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. In the course of processing of the source web pages for the purposes of crawling, analysing and indexing, personal data does not manifest itself as such in any particular way.[12]

He further observed that:

> the internet search engine service provider cannot in law or in fact fulfil the obligations of controller provided in Articles 6, 7 and 8 of the Directive in relation to the personal data on source web pages hosted on third-party servers. Therefore a reasonable interpretation of the Directive requires that the service provider is not generally considered as having that position.[13]

Professor Anne Debet, also a former Commissioner with the French Data Protection Authority (CNIL), recently asked the following question[14]:

> How does Google respect the Directive's grand principles: proportionality, fair and lawful data collection, limitation of the retention period? How can it respect the rules requiring previous formalities (authorizations for processing of some sensitive data, etc.) and notifications? The search engine activity implies that Google is potentially responsible for all of the content published on the Internet as a controller.[15]

In February 2013, some publication already reflected on the 'impossible obligations'[16] to which search engines would be potentially subject if they were categorized as data controllers. As an illustration, the principle of prohibiting the processing of sensitive data within the meaning of the Directive's Article 8, that is disclosing the racial or ethnic origin, political or religious opinions, or the sexual orientations of the data subjects, 'present difficulties for search engines. Indeed, many websites, blogs and profiles on social networks include such information, which the search engines index'.[17] Consequently, 'if such activities constituted processing of personal data, then search engines would be structurally and continuously in violation of European legislation'.[18] It should be remembered that, in the *Google Spain* case, the Advocate General was himself opposed, 'undoubtedly for good reason',[19] to categorizing search engines as controllers.[20] However, the Court decided otherwise. But in so doing, it did not demarcate, far from it, all of the consequences resulting from this decision.

The third reason why the *Google Spain* judgment is so noticeable stems from the fact that the data subject's rights to rectify and to oppose the processing of his data, as provided under the Directive's Articles 12 and 14, is construed as the right to get the search engine to deindex him from the list of results of web links displayed as the result of a search performed based on the data subject's name. The Court specified that this right to be deindexed is also applicable 'even, as the case may be, when its publication in itself on those pages is lawful'.[21]

Nonetheless, and in accordance with its case law on proportionality,[22] the CJEU has ruled that the RTBF is not an absolute right. It must be reconciled with other fundamental rights, of the same rank, such as freedom

8 Within the meaning of art 4 of the Directive.

9 *Google Spain* judgment (n 5) para 57.

10 Kuner (n 2) 10.

11 Case C-131-12, Opinion of AG Niilo Jaaskinen, delivered on 25 June 2013, para 84.

12 Ibid.

13 Ibid, para 89.

14 All translations from French- and Spanish-language materials have been made by the author.

15 A Debet, 'Google Spain: la suite, encore des questions pour la CJEU' [Google Spain: The Next Step, More Questions for the CJEU], Communication Commerce Electronique (2017) no 4, 42.

16 Y Padova and D Lebeau-Marianna, 'Entre droit des données personnelles et liberté d'expression, quelle place pour les moteurs de recherche?' [What Role Do Search Engines Have Between Personal Data Law and Freedom of Speech?] Lamy du droit de l'immatériel (LRDI) (February 2013) no 90, 71.

17 Ibid.

18 Kuner (n 2) 10.

19 Debet (n 15) 39.

20 Opinion of AG Jaaskinen (n 11) paras 80–83.

21 *Google Spain* judgment (n 5) para 88.

22 The principle of proportionality is both a general legal principle (Case 265/87 *Hermann Schräder HS Kraftfutter GmbH & Co KG contre*

of expression[23] and information.[24] In this case, the Court stated that:

> inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, . . . a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.[25]

There are many unresolved questions about the practical application of the RTBF. What is the 'role played' by the data subject in public life? For example, is this term interpreted consistently within the European Union (EU) although the national cultures are so different in terms of transparency of public life? What are the other 'fundamental rights' to take into consideration? Do the national courts, and the data protection authorities, which are interestingly also competent after the Court's judgment, develop the same interpretation of how to balance interests?

These three particular features of the *Google Spain* judgment appear to give rise to several legal uncertainties. First of all, there is uncertainty as to the territorial scope of the RTBF; secondly, uncertainty as to the obligations that are enforceable against the search engines categorized as a 'controller'; and, thirdly, uncertainty as to the rights to be taken into consideration to balance interests and as regards the consistency of interpretations developed by the courts and data protection authorities, respectively.[26]

It is in light of this that the French Council of State's 11 preliminary questions may be best viewed. Resulting from different cases, these questions may be grouped into two categories. The first category is related to the consequences of categorizing search engines as controllers with respect to what the Directive's Articles 8 and 9 prohibit them from doing, collecting, and processing 'sensitive data and data involving an offence'. But, as Professor Anne Debet observes, 'it is difficult to see on what exemption ground Google's processing of personal data could be based'[27] and points out that 'the application of all of a controller's obligations and responsibilities to search engines has the effect of a very poorly and ill-conceived legal solution, although one cannot see any solutions to these difficulties'.[28] According to the French Council of State itself, a literal application of the prohibition provided for in the Directive's Articles 8 and 9 would have 'excessive consequences'[29] on search engines and, one may add, on how the Internet functions in general. It is now up to the Court, which is now in a situation where it has to rule on its own case law, from the EU's Charter of Fundamental Rights,[30] to find a bespoke solution for this cul-de-sac.

The second category of questions involves the territorial scope of the right to be deindexed resulting from the dispute between Google and the French Data Protection Authority (the 'CNIL'), which fined the search engine €100,000.[31] This category of questions suggest three possible choices to the Court: (i) must the right to be deindexed be interpreted in the sense that, when enforced, it must apply to all of the domain names (.com, .fr, .ca, etc.), 'regardless of the place from which the search is performed with the searcher's name, *including outside of the Directive's territorial scope*?'[32] (emphasis added). As it would involve all domain names and would make no distinction to the data subject's location, this first option will be called 'universal'.[33]

In case of a negative response, (ii) must the right to be deindexed apply only to the results displayed based on a search on the domain name corresponding to the State where the search is deemed to have been launched[34] or more broadly on the domain names that

Hauptzollamt Gronau ECLI:EU:C:1989:303) and a European constitutional principle pursuant to art 5 s 4 of the Treaty on the EU ('TEU'), which provides as follows: 'Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.'

23 See M Fazlioglu, 'Forget Me Not: The Clash of the Right to be Forgotten and Freedom of Expression on the Internet' (2013) 3 (3) IDPL 149.

24 Art 11 of EU Charter of Fundamental Rights (2000/C 364/01).

25 *Google Spain* judgment (n 5) para 81.

26 As regards the question of the complementarity or competition between the courts' jurisdiction and the one of the data protection authorities in the balance of interests called upon by the practical implementation of the right to be forgotten, see Y Padova 'Le droit à l'oubli, un droit universel?' [The Right to be Forgotten, a Universal Right ?], LRDI (October 2016) no130, 45ff.

27 Debet (n 15) 40.

28 Ibid 42.

29 Series 1 (n 3) para 22.

30 A Bretonneau, 'Le droit au déréférencement en huit questions' [The Right to Deindexation in Eight Questions], Droit Administratif (June 2017) no 6, 972, end note.

31 CNIL's deliberation no 2016-054 of 10 March 2016 imposing a fine on company X (Google).

32 Series 2 (n 3), art 2 1.

33 Padova (n 26) 35.

34 '.fr' for a French person, '.uk' for a British person, etc.

correspond to all of the EU Member States. This option will be called 'regional' here.

Lastly, (iii) must the right to be deindexed be interpreted to mean that, when enforced, the search engine is required to delete, from an IP address deemed to be located in the data subject's State, all of the disputed links for all of the relevant domain names, including those outside the EU like '.com'? This outcome, referred to as geoblocking, has mixed characteristics because it borrows from the universal outcome the fact of being applicable to all of the existing domain names while simultaneously limiting its territorial effect by demarcating it by locating the user's IP address.[35] This option, which is both global and local, is called here 'glocal'. Within the framework of the sanction procedure before the CNIL, Google offered to implement such technical proposal. Though the CNIL considered it as an improvement, it finally judged it insufficient and, as a result, fined the search engine company.[36]

But, it would be wrong to consider that these two categories of preliminary questions are not related, quite to the contrary. The choices made in one category are likely to amplify, or limit, the effects of the choices made in the other category. 'The question of the territorial scope of the deindexation, which is separate from the question of its substantive scope, reverberates with it',[37] as the Public Rapporteur rightly notes in her observations.

Hence, first, the convergence of a pure, simple prohibition for search engines to process sensitive data, with, secondly, an automatic right to be deindexed at the data subject's request, greatly increases the effect of the RTBF, which would become 'vertiginous'[38] according to other authors.

This is because certain online data, the collection of which is prohibited in Europe:

> can be collected on websites the responsible parties of which are not governed by the directive geographically. Considering that a search engine like Google, which geographically may fall within the territorial scope of the [Directive's], is prohibited from indexing such data amounts to clearly lowering Internet users' accessibility to content on the Internet that is not regulated by European Law.[39]

In other words, the 'excessive'[40] consequences of applying the Directive's Articles 8 and 9 to search engines, as the French Council of State fears, would be all the more excessive because such application would be 'universal'.

This article mainly focuses on the CJEU's possible positions as to the territorial scope of the RTBF following the submissions of preliminary questions by the French Council of State and as such relies predominantly on French legal sources and literature. However, international and European aspects will be discussed in order to illustrate the arguments developed.

Given these considerable stakes, this article proposes to concentrate on the territorial consequences of each of the three options submitted to the Court, the universal and regional, the 'glocal', while previously pointing out the questions not submitted to the Court, which are nonetheless of great interest.

Questions not submitted to the court: the notion of 'single processing operation' and the effect over time of the RTBF

The 11 preliminary questions sent to the Court are of great importance, but some questions that have not been submitted are of equal interest. Two of them are particularly relevant here: the notion of single processing as a legal and technical basis for extraterritoriality and the question of the effect over time of deindexation.

Single processing, as a legal and technical basis of extraterritoriality, will not be examined by the CJEU

One of the principal lessons of the CNIL's decision to issue a fine, which is the basis of the second category of preliminary questions, is the finding that the search engine 'is *single processing* endowed with multiple technical access paths'[41] (emphasis added), which are its various national extensions.

This point is essential[42] because it is the legal basis of the CNIL's request vis-à-vis Google Inc. to deindex all of the search engine's extensions, including Google.com. Indeed, if the extensions.com (USA), .ca (Canada), and .au (Australia) are all based on a single processing operation, then any search performed from one of these countries is based on the same processing operation as the processing from France (.fr). Consequently, as the CNIL

35 The Internet Protocol address, or the IP address, is the number that identifies each computer connected to the Internet, or more generally and specifically, any IT hardware (router, printer) interface connected to an IT network using the IP.

36 CNIL's deliberation no 2016-054 (n 31).

37 Observations of the Public Rapporteur Mrs A Bretonneau, RFDA, 2017, 972ff and seq.

38 Odinet and Roussel (n 6) 742.

39 Bretonneau (n 30), end note.

40 Series 1 (n 3) para 22.

41 CNIL's deliberation no 2016-054 (n 31).

42 Padova (n 26), 37–38.

has jurisdiction over the latter processing operation, it also has jurisdiction for all other searches performed from any of the search engine's existing extensions because it involves a 'single processing operation'.

In summary,[43] a search engine combines multiple processing operations that are divided into two large categories: the first category consists in compiling and indexing all of the information accessible to the public on the web, and the second category consists in responding to the individual requests and searches in order to display their results. The first category is systematic, whereas the second category is specific and customized.

Considering that the search engine represents a single processing operation and that such search engine is a 'controller' within the Directive's meaning, this results in making all of its operations subject to European law and not only some among them. In doing this, this reasoning constitutes an obstacle to a solution that would have constituted in distinguishing between processing operations and, therefore, enabling the possible emergence of a differentiated and localized legal and technical response to the right to be deindexed.

Indeed, by considering that two processing operations exists the first one being systematic (indexing the web) and, as such, partially avoiding European data protection law (both its substantive and territorial provisions) and the second one being specific, displaying the results for end users, it would have been possible to reconcile compliance with European law in the final result that is visible for such European users, without destabilizing all of the search engines' indexing activities.[44]

Unfortunately, the French Council of State did not explore this path. While noting that the search engine, 'executes several successive operations, including the indexing of content present on the web and making such content available to Internet users based on a given order of preference',[45] the Council of State found that, in any case, such situation, 'is not an obstacle to being regarded as a single processing operation'.[46] The Council of State's demonstration is at the very least succinct although the Public Rapporteur provides much more support for her comments.

After having broken down the details of the many phases through which a search engine works before displaying the result to the Internet user, the Public Rapporteur cites as evidence the definition of personal data processing[47] of Article 2 of both the Directive and of the French Act on Information Technology, 'any operation or set of operations' to rule out 'sequencing' and, hence, the existence of several processing operations. Continuing her demonstration, the Public Rapporteur argues that, 'the differentiation of results, a process that begins at the stage of forming the pre-list, depends on a multiplicity of factors, among which the domain name plays only a marginal role, such that if one had to count as many processing operations and displays, then there would be as many processing operations as there are Internet users'.[48]

This hypothetical situation, which was clearly ruled out by the Public Rapporteur, had been contemplated by the Article 29 Working Party (WP29)[49] itself in 2008, within the framework of its opinion on search engines.[50] Wondering about categorizing search engines as controllers, the WP29 observed that 'Search engine users could also be considered as controllers, but their role will not be based on the directive because they involve only personal activities.'[51]

In its request sent to the Court, the French Council of State simply states that, if the results can differ depending on the domain name from which the search is performed on the search engine, which is nevertheless a significant fact that may attest to the existence of several processing operations, 'it is clear that the links displayed in response to a search come from a shared database and indexing work'.[52] As Chabert observes, 'the obvious fact that there is a single processing operation should have merited being built upon, because the geolocalization technology appears to reflect a

43 Opinion of Advocate General Niilo Jaaskinen (n 11) para 73: 'Google's search engine's crawler function, called "googlebot," crawls on the internet constantly and systematically and, advancing from one source web page to another on the basis of hyperlinks between the pages, requests the visited sites to send to it a copy of the visited page. The copies of such source web pages are analysed by Google's indexing function. Sign strings (keywords, search terms) found on the pages are recorded in the index of the search engine. Google's elaborate search algorithm also assesses the relevance of the search results. The combinations of these keywords with the URL addresses, where they can be found, form the index of the search engine. The searches initiated by the users are executed within the index. For the purposes of indexing and displaying the search results, the copy of the pages is registered in the cache memory of the search engine.'

44 And, consequently, circumscribing the potentially 'excessive' consequences of the right to be forgotten.

45 Series 1 (n 3) para 2.

46 Series 1 (n 3) para 10.

47 Defined in Articles 2 of the Directive and of the French 'Act on Information Technology, Data Files and Civil Liberties' of 6 January 1978.

48 Bretonneau (n 37) 974.

49 The Working Party created pursuant to Article 29 of Directive and which federates the data protection authorities of the Member States (hereinafter, the 'WP29').

50 WP29 Opinion 1/2008 on data protection issues related to search engines adopted on 4 April 2008, 15.

51 Ibid 14.

52 Series 2 (n 3) para 11.

"differentiated" processing operation, if not by the language, then at least by the search purpose, country or region'.[53] Here, one can regret the 'missed opportunity' of questioning the Court about this essential point.

Could the vagueness of the effect over time of the RTBF be considered as a 'perpetual' commitment?

Supposing that the search engines grant a data subject a removal from web links in accordance with his right to be deindexed, for how long must this result last? Is this an infinite deindexation or is it limited in time? This question was not addressed, either in the *Google Spain* judgment, or in the CNIL's decisions imposing fines, or in the Council of State's preliminary questions. However, the analogy with other branches of law where blocking or filtering measures[54] exist show that this question is of great relevance.

For example, in terms of blocking the access to unlawful content, in two important judgments,[55] the CJEU has ruled that creating a block towards illegal content, as ordered by a court, had to be limited in time. Otherwise, it would be disproportionate.[56]

Of course, the right to be deindexed does not require that the links, which removal is being requested, redirect to unlawful content because this right is applicable, even when the source website's data processing 'is lawful',[57] stated the Court. Moreover, the RTBF does not make the disputed content disappear; it remains visible on the original website, but it limits access through the results of searches performed on search engines. This being the case, if access to an unlawful website and, therefore, to the content that harms individuals' rights even more, can only be made inaccessible for a limited period, is it not paradoxical that the deindexation to a site with lawful content, and therefore, by definition which harms individuals' freedoms to a lesser extent, has no limit in time?

This difference in the effect over time mainly results from the Court's assessment of the balance of interests at stake. Thus, in its *Sabam v Netlog* judgment, the Court states, conventionally, 'the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights'.[58]

In *Sabam v Netlog*, the Court also considers that national authorities and courts, 'must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as hosting service providers pursuant to Article 16 of the Charter'.[59] Yet, 'the injunction requiring the installation of the contested filtering system involves monitoring all or most of the information stored by the hosting service provider concerned, in the interests of those right holders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also works that have not yet been created at the time when the system is introduced'.[60]

Such an injunction would lead to a violation of the freedom to conduct a business, since 'it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense',[61] which requires that, 'measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly'.[62] Within this context, the Court concludes that:

> it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as hosting service providers.[63]

The question of the 'cost' of the deindexing measures was never addressed by the search engines, nor, consequently, was it examined by the Court. Perhaps the volume of deindexation requests, combined with the fact that they are not limited in time, could in the long run change this situation and, hence, the balance of interests as determined today by the Court.

Furthermore, the Court recently developed a more restrictive interpretation of the scope of the right to be deindexed. In this case, it balanced it with the principle of the 'legal certainty' of third parties for which legal

53 C Chabert, 'Quelle portée pour ce fameux droit à l'oubli des moteurs de recherche' [What Scope for Search Engines' Renowned Right to be Forgotten], LRDI (March 2017), no 135, 3.

54 As Professor L Marino explains, 'technically, Internet filtering is a set of technologies that limit access to certain websites. Blocking is a category of filtering. It is strict filtering, which stops traffic', Jurisclasseur Communication, Responsabilités civiles et pénales des fournisseurs d'accès et d'hébergement [The Civil and Criminal Liability of Access and Hosting Providers], booklet 670, para 62.

55 Case C-360/10 *Sabam v Netlog* ECLI:EU:C:2012:85 and Case C-70/10 *Scarlet v Sabam* ECLI:EU:C:2011:771.

56 Ibid.

57 *Google Spain* judgment (n 5) para 88.

58 Case C-360/10 *Sabam v Netlog* (n 55) para 42.

59 Ibid, para 44.

60 Ibid, para 45.

61 Ibid, para 46.

62 Ibid.

63 Ibid, para 47.

grounds were sector regulations related to the trade register.[64] The Italian Supreme Court referred the matter to the Court, asking whether the principle of limiting in time the retention of personal data as provided for by the Directive, here involving the data of the company's executives/officers in the trade register, had 'to take precedence'[65] over the principle of publishing such data without a limitation in time, as provided by another Directive[66] and conceived as a guarantee of enforceability of third parties' rights.

The Court responded negatively, finding that, 'in principle, the need to protect the interests of third parties in relation to joint-stock companies and limited liability companies and to ensure legal certainty, fair trading and thus the proper functioning of the internal market take precedence'.[67] The Court does, however, provide some nuance to this precedence 'in principle' of the third parties' right to legal certainty as related to the right to be deindexed. The Court indicates that it:

> cannot be excluded, however, that there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon expiry of a sufficiently long period after the dissolution of the company in question, to third parties who can demonstrate a specific interest in their consultation.[68]

Here again, it cannot be excluded, however, that over time, because the 'role' of a person will have changed, for example, by becoming public, or because the balance of the interests at stake will be assessed differently, that the effects of the right to be deindexed will turn out to be limited in time.

In addition, the time factor plays a role in the very assessment of the balance of rights, as for instance, where the 'original publication of a piece [of information] is legitimate, but its continuous accessibility becomes, after a certain time, unlawful, since the public's interest in accessing the piece has diminished to such an extent that it is outweighted by the data subject's privacy interests'.[69]

One can only regret that time considerations in relation to the right to be deindexed are not part of the questions submitted to the Court, as effect in time of such right will necessarily be a question of great importance for the entities that have to comply with deindexation orders.

Presentation and consequences of the 'universal' or 'regional' options of the RTBF

The universal option is defended by the CNIL, in its fine issued against Google and by the WP29. The WP29 stated that:

> In order to give full effect to the data subject's rights as defined in the Court's ruling, delisting decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting delisting to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the ruling.[70]

The WP29 added, 'in practice, this means that, in any case, de-listing should also be effective on all relevant domains, including .com'.[71]

Therefore, it appears as if it is the legitimate fear of the '*circumvention*' of European law and the subsequent weakening of the protection offered to data subjects that constitutes the WP29's main motivation in favour of the universal option. This being the case, can this objective, with which everyone agrees, be served by means other than universal extraterritoriality?

The European regulators appear to be more nuanced than the WP29's opinion would make one believe, and they actually appear to be divided on this question.[72] For instance, the Spanish Data Protection Authority (DPA), though at the origin of the Costeja decision, has expressed 'doubts about the interpretation' of the CJEU judgment 'as to its scope'. Indeed, this DPA considers[73] that:

> the effectiveness which the correct application of the Judgment requires can only be achieved if the blocks on the results list of the search engine occur, when searches are performed *from the territorial ambit within which the*

64 Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* ECLI:EU:C:2017:197, para 50.

65 Ibid, para 29.

66 Principle provided for in accordance with Directive 68/151 EEC, art 3.

67 Case C-398/15 (n 64) para 60.

68 Ibid.

69 G Sartor, 'The Right to be Forgotten in the Draft Data Protection Regulation' (2015) 5 (1) IDPL 64, 70.

70 WP29 Guidelines on the Implementation of the CJEU Judgment on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez' C-131/12, adopted on 26 November 2014, 3.

71 Ibid; It should be pointed out briefly that the current practice of search engines, and of Google in particular, is to deindex the content on all of the search engine's extensions, including .com when the request appears to come from the requesting party's country, with the country being determined as a priority by the user's IP address.

72 Hence, the ICO, the British data protection authority, and the Spanish data protection agency have different opinions that favour the 'glocal' option. See Padova (n 26).

73 Spanish Data Protection Agency, Expediente No E/02887/2015, Resolución de archivo de actuaciones, 2015, 7.

> *Judgment, and the legislation to which this Judgment refers, among other things, is applicable because it is within this territorial framework where, as a general rule, the impact of those results is generated upon the rights of the parties concerned* as a result of the universal accessibility and availability of certain information through name specific searches in the search engine[74] (emphasis added).

And the Spanish DPA states that the step implemented by Google Inc. is '*necessary and proportionate to the purpose sought, since it aims to block results only when the search requests are made from the territorial ambit within which the Judgment and the related legislation are applicable*, and the rights and interests of the parties concerned may be directly affected'[75] (emphasis added).

The Spanish DPA concludes its assessment by considering that:

> in accordance with the criterion of interpretation used by the WP29 concerning the CJEU judgment and taking into account the argument raised by Google Inc. ... the necessary steps have been taken by Google Inc. so that, *when carrying out a search in Spain* containing the names of the complainants, the search engine results page does not display the websites mentioned in the complaint *in any of the versions of the search engine accessible from Spanish territory*[76] (emphasis added).

Similarly, the UK DPA, the Information Commissioner's Office (ICO), ordered Google to delist search results accessible by Internet users from the UK. In this context, the ICO required the delisting of search results where the processing carried out by Google Search in order to produce the requested results were carried out in the context of the activities of Google UK Ltd, or any other Google company established in the UK, and, in particular, for the purpose of advertising content promoted or sold by those companies and whose recipients are residents of the UK. Considering the way Google delivers content, the ICO considered that delisting must be implemented on all versions of Google Search service directly accessible from within the UK.[77]

As noted by Julien Leclainche:

> Twenty-four independent authorities considered that this reaction [the steps taken by Google Inc. previously mentioned] was sufficient whereas the English, Spanish and Portuguese authorities requested to take into account the geographical origin of the request. The CNIL is the only authority to require global delisting on all domain extensions used by Google.[78]

Hence, there is still a consensus to be reached between the authorities[79] with respect to the territorial scope to be granted to the RTBF.

The significant stakes of the 'universal' option

As the French Council of State indicates, the universal option ends with the disputed links no longer appearing, 'including outside the Directive's territorial scope'.[80] This is why this option has a very powerful extraterritorial effect, on which much lively debate is based.

The wording used by the Council of State seems somewhat surprising. How can legislation, here Directive 95/46, have a legal effect outside its own territorial scope, where this scope has been defined by this text itself? Is the question not rather that the Directive has 'undesirable' extraterritorial effects, as the WP29 itself [81] refers to them, which the Court should not exacerbate?

Substantively, as Professor Bruguière forcefully expressed regarding the WP29's position:

> one cannot imagine a French court imposing, based on French law, interpreted in light of European Union law, a deindexation measure on a foreign version like Google.com. If the opposite outcome were adopted, Americans would be deprived of accessing information on their own search engines based on a law that is completely unrelated to them and knowing that they favor even more than we the public's right to information. Add to this that, if each court claims that its law is universal, the national injunctions would run a great risk of bumping into each other rather quickly.[82]

Conversely, Professor Debet argues that 'if one considers that Google does not have the right to process sensitive data or data related to offenses, it must deindex regardless of the legal regime and the law to which the indexed website may be subject'.[83] However, as stated

74 Ibid, 9.

75 Ibid, 9–10.

76 Ibid, 10.

77 Information Commissioner's Office, Enforcement notice, 18 August 2015.

78 J Leclainche, 'Droit à l'oubli, droit international et droit à l'information' [Right to be Forgotten, International Law and Right to Information], Les Echos (30 May 2016).

79 Debet also considers that the CNIL 'goes too far by refusing filtering based on IP address': A Debet, Droit au déréférencement: suite du bras de fer opposant Google à la CNIL [Right to be Forgotten, Next Step on the Fierce Battle between Google and the CNIL], Communication Commerce Electronique, no 7–8, July 2016, 67.

80 Series 2 (n 3) para 16.

81 WP29, Opinion 8/2010 on applicable law, adopted on 16 December 2010, 24.

82 J Bruguière, 'Droit à l'oubli numérique des internautes ou ... responsabilité civile des moteurs du fait du référencement ?' [Internet Users' Right to be Forgotten or the Search Engine's Civil Liability due to Indexing], Communication Commerce Electronique, 2015, no 5, study 10, para 33.

83 Debet (n 15) 42.

by Kuner, EU data protection law may be 'construed broadly in order to protect against its circumvention, but there must be some limits to its territorial application, if it not to be universally applicable to the entire Internet'.[84]

Although in the national judiciary system, the courts' decisions are self-enforcing beyond their original jurisdiction, at the international level, they are automatically self-enforcing only in the territory of the relevant State. Therefore, the enforcement of a decision stops at the border, 'a frustrating situation for the litigant', as Professor Ancel accurately emphasizes.[85] But why would it be any different with the right to be deindexed?

Of course, as recognized by the US Supreme Court, the Internet is 'fundamentally and profoundly anti-spatial, [because] one cannot say where it is located or describe its form or proportions, one cannot say to someone how to go there. But, one can find things on the Internet without knowing where they are. The Internet is ambient.'[86] Can one infer from this characteristic of ubiquity that the notion of territory and of territorial jurisdiction resulting therefrom disappear? It is one thing to observe that the Internet 'presents a challenge to the States' regulatory power and scrambles certain established legal principles, such as that of a standard's territoriality',[87] and it is quite another to consider that a rule created by European case-law must apply in an extraterritorial and universal fashion.

The question of extraterritorial effects of the universal option is even more important where third party States potentially impacted do not have similar laws and rules on the relevant matter. As pointed out by some authors in relation to the application of the *Google Spain* judgment is the concept of harmonization: 'the higher the degree of harmonization between the States, the less problematic an extra-territorial assertion of jurisdiction becomes'.[88] This is particularly relevant for the USA where data protection law not only lacks uniformity as it is based on both federal and state laws but also does not provide for the same rights to individuals than the Directive. This aspect, which relates to the international law principle of reciprocity, surely weights against the legitimacy of European courts in imposing deindexation orders on a universal basis.

The founding European legislation clearly provides that the treaties apply to the Member States[89] and, therefore, *a fortiori* to their territory and not beyond it. Similarly, European courts have clearly established that a unilateral act of the EU cannot create rights and obligations outside the territory as defined.[90] In its *Bodil Lindqvist* judgment, the Court already ruled that the Directive must not be interpreted in such a fashion that it would apply to the entire Internet. Otherwise added the Court, this could lead to a situation where the '*Member States would be obliged to prevent any personal data being placed on the internet*'[91] (emphasis added).

In addition to the fact that the universal option could turn out to be contrary to the traditional rules of public international law[92] and country's sovereignty, it would automatically increase 'the risks of conflicts in standards of the seedling that is the universality of the network that interconnects individuals belonging to separate legal systems'.[93] As doctrine states, the effects of the universal option would be 'as drastic',[94] both 'technically' and 'politically', and it would contradict 'a cardinal notion of Internet law: the criterion known as targeting'.[95] It would also be unique in national legal systems, which only very rarely, and in serious situations, confer such extraterritorial scope.

The singularity of the 'universal option'

Extending the applicability of the right to be deindexed to the entire world would confer on it a scope greater

84 Kuner (n 2) 12.

85 Ancel in D Alland and S. Rials, *Dictionnaire de la culture juridique* [*Dictionary of Legal Culture*], Droit International Privé, Paris: Lamy PUF, 2003, 496.

86 United States Supreme Court, *Reno v/ ACLU*, 26 June 1997, cited by B Barraud, 'Etat territorial face au cyberspace mondial' [The Territorial State Confronted with the International Cyberspace], LRDI (January 2016) 43.

87 2014 Annual Study of the Council of State, '*Conseil d'Etat, le numérique et les droits fondamentaux*' [French Council of State, Digital Technology and the Fundamental Rights], La Documentation Française (2014) 37.

88 B Van Alsenoy and M Koekkoek, 'Internet and Jurisdiction after Google Spain: the Extra-Territorial Reach of the EU's Right to be Forgotten', KU Leuven, Leuven Centre for Global Governance Studies Working Paper No 152, March 2015, 27 https://ghum.kuleuven.be/ggs/publications/working_papers/2015/152vanalsenoykoekkoek.

89 Art 52 of the TEU, which refers to art 355 of the Treaty on the Functioning of the European Union.

90 Case T-212/02 *Commune de Champagne, Défense de l'appellation Champagne ASBL and Cave des Viticulteurs de Bonvillars v Council of the European Union and Commission of the European Communities* ECLI:EU:T:2007:194, paras 89–90.

91 Case C-101/01, Criminal proceedings against Bodil Lindqvist ECLI:EU:C:2003:596, para 69: 'If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a 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 there 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. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.'

92 Hence, the charter of the United Nations stipulates in art 2(1) that 'The Organization is based on the principle of the sovereign equality of all its Members.'".

93 Bretonneau (n 37) 976.

94 Chabert (n 53) 4.

95 Ibid.

than that which is applicable to a number of other legal disciplines, like French criminal law. Hence, Article 113-7 of the French Criminal Code provides that French law applies to any crime or any misdemeanor punished with incarceration committed by a French national or a foreigner 'outside of French territory when the victim is a French national'. This universal jurisdiction, referred to as 'passive', is 'highly criticized' as observe some authors,[96] who are not suspected of being hostile to data protection. With exceptional application, universal jurisdiction is subject to the condition of the victim's nationality. This criterion, therefore, reinforces the importance of a national link between the applicable law and the relevant person, a link that would indeed disappear if the universal option of the right to be deindexed were to prevail.

In its 'universal' sense, the right to be deindexed would benefit from an even broader territorial scope as the scope recognized for punishing facts that are more serious by nature. As the authors cited *supra* observe, 'many questions arise involving the conflict between the criteria for application of directive 95/46 and the Act on Information Technology and Civil Liberties and the criteria for applying criminal law, including French criminal law'.[97]

Hence, under French criminal law, only certain particularly serious offences, such as felonies and misdemeanors that infringe national fundamental interests mentioned in Article 113-10 of the same code, are subject to the jurisdiction of French criminal law regardless of the defendant's nationality. Here again, a comparison with the universal scope of the RTBF is instructive. Indeed, why would less serious acts, which may even be legal since the right to be deindexed does not require the disputed content to be unlawful, benefit from legal protection that is broader in territorial terms than acts that are illegal and, hence, by nature, more serious?

In addition, pursuant to the provisions of Article 113-2 (2) of the French Criminal Code, 'the offense is deemed to have been committed in the Republic's territory when one of its acts took place in the territory'. In other words, French criminal law applies if the substantive element of the offence was committed, in whole or in part, in the Republic's territory.[98] As regards offences committed on the Internet, the French Supreme Court has ruled that the offence was deemed to have been committed in any place where the alleged comments were received, but that 'French criminal law's role is not to apply universally, the disputed website pages had to be intended for the French public for the law to be legally implemented.'[99] In other words, it did not suffice that the website was accessible in France for the offence to be deemed to have been committed in France.[100]

The legislature recently extended[101] the notion of an offence deemed to have been commitment in French territory. Indeed, the new Article 113-2-1 of the French Criminal Code provides that: 'Any felony or misdemeanor committed through an electronic communication network, when it is attempted or committed against a natural person residing in the Republic's territory or against a legal entity whose registered office is located in the Republic's territory, shall be deemed to have been committed in the Republic's territory.' This provision is assuredly innovative in that the offence is deemed to have been committed in the Republic's territory not due to the location, in France, of one of the elements constituting the offence, but with respect to the victim's place of residence or establishment.

Of course, Directive 95/46, in its recital 21, indicates that it 'is without prejudice to the rules of territoriality applicable in criminal matters'. This being the case, the coherence of our legal systems and their proper structuring contributes to the legal certainty for natural persons and companies and to the foreseeability of law, principles to which the Court is particularly vigilant. There is no doubt that its decision on the territorial scope of the RTBF, which was eagerly awaited, will have some effect in this field.

The uncertain applicability and enforceability of the 'universal option'

Professor Carbonnier pointed out that the wider a territory is, the more ineffective the standards governing it become.[102] The right to be deindexed, in its universal meaning, is not an exception to this rule. As stated by Kuner, the *Google Spain* judgment 'provides a strong affirmation of online data protection rights, but fails to indicate a way forward for their effective implementation and realization, the development of which will likely to be a struggle for data controllers, DPAs and

96 J Massot, A Debet and N Metallinos, 'Informatique et Libertés' [Information Technology and Civil Liberties], Lextenso editions (2015) 211.

97 Ibid 210.

98 Cass crim, 7 January 2014, no 12-80.024: JurisData no 2014-000023.

99 N Rias, 'Principes généraux de la loi pénale' [General Principles of Criminal Law], Jurisclasseur Pénal, para 45.

100 Cass crim, 12 July 2016, no 15-86.645: JurisData no 2016-013713.

101 French Act no 2016-731 of 3 June 2016.

102 J Carbonnier, 'Théorie sociologique des sources du droit' [Sociological Theory of the Sources of Law], Association corporative des étudiants en droit de l'Université Panthéon Sorbonne, 1961, 150.

courts'.[103] The preliminary questions sent to the CJEU are the very illustration of these shortcomings.

Indeed, how effective and operationally applicable will a universal RTBF be? 'Wanting extraterritorial application of legislation is not always sufficient; one must also have the means for making the decisions obtained apply',[104] the doctrine rightfully observes. Yet, this is not easy at all and the precedent of the *Yahoo* Auctions case,[105] still in everyone's mind, taught us to be careful, if not modest.

As regards the data protection authorities' powers to intervene, in the *Schrems* case, the CJEU pointed out that the authorities 'do not have powers on the basis of [the Directive's] Article 28 in respect of processing of such data carried out in a third country'.[106] And the Court added in the Weltimmo case that:

> it follows from the requirements resulting from the relevant Member State's territorial sovereignty, from the principle of legality and from the notion of the rule of law that the enforcement power cannot, in principle, be exercised outside of the legal limits within which an administrative authority is authorized to act, in compliance with the law of its Member State.[107]

Of course, thanks to the Court's case law in its *Google Spain* and *Weltimmo*[108] cases, these authorities can punish a controller whose subsidiary constitutes an establishment, which, within the framework of its business, participates in the disputed processing of personal data. However, what would be the outcome in another hypothetical situation, which does not exist in the French case involving Google, but exists in other Member States, in which the controller has no establishment in the territory of the relevant State? In such case, the controller located outside of the EU must designate a 'representative'.[109] Yet, what responsibility does this representative have with respect to plaintiffs' individual requests and vis-à-vis the supervisory authority. What effective intervention power does he have on processing? Can he be punished for failures committed by the controller?

Nothing is less certain, as illustrated by the arguments devoted to this question in 2010 by the WP29:

> the question of enforcement against a representative raises practical issues, as shown by Member States' experience. This would be the case if for instance the only representative of the controller within the EU is a law firm. There is no uniform answer in national implementing provisions to the question whether the representative can be held responsible and sanctioned, on a civil or criminal basis, on behalf of the controller. The nature of the relationship between the representative and the controller is decisive here. In some Member States, the representative substitutes for the controller, also with regard to enforcement and sanctions, while in others it has a simple mandate. Some national laws explicitly foresee fines applicable to the representatives, while in other Member States this possibility is not envisaged,[110]

which is the case in France.

Even though the representative may be sanctioned on behalf of the controller located outside of the EU, this may convey the risk of 'discouraging any legal entity or natural person established in France from accepting such liability?'.[111] This question should not be put aside.

The regional option, an attempt to create a form of digital territoriality

The 'regional' choice is an attempt to recreate a form of digital territoriality through a group of domain names. As a result, it has led to relatively little commentary. This option would lead to a situation where the right to be deindexed, when granted to the data subject, leads to deleting the accessible links that are accessible only from his presumed national extension, or, more broadly, from all of the 'European' extensions.

This option can be an interesting outcome, given Google's implementation of the 'redirection' technology for searches performed by Internet users. Google's default settings now automatically redirect Internet users in France to the website google.fr even though they have entered the google.com address in their browser. According to the information provided by Google to the Spanish DPA,[112] this process now allegedly leads to 'less than 3% of searches performed from Europe (which includes the EU and the EFTA) use the search engine's non-European extensions'.[113] This means that '97% of searches performed in Europe by European Internet users display results which, if need be, will have

103 Kuner (n 2) 21.

104 Massot, Debet and Metallinos (n 96) 217.

105 Interim Order of 20 November 2000, *Yahoo v LICRA and UEJF*, Paris Civil Court.

106 Case C-362/1 *Maximillian Schrems*, ECLI:EU:C:2015:650, para 44.

107 Ibid, para 56.

108 Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* ECLI:EU:C:2015:639, para 3.

109 Pursuant to the provisions of art 4 of the Directive and art 2 of the General Data Protection Regulation.

110 WP29's 2010 Opinion (n 81) 27.

111 Massot, Debet and Metallinos (n 96) 217.

112 Spanish DPA, Expediente No E/02887/2015 (n 73).

113 Ibid 3.

been modified in accordance with the implementation of the Costeja judgment',[114] as interpreted by Google.

The strength of the regional option resides in its consistency with regard to the European nature of the right to be deindexed. First, it reminds the European origin of the right to be deindexed (the Directive). Secondly, it is in line with the case law interpretation by the highest judicial authority of the EU (the CJEU) according to which the RTBF is not an absolute right. Lastly, the 'digital territory' in which the right to be deindexed would apply corresponds to the physical territory of the EU. Therefore, it appears to be strongly coherent because it re-establishes a link between the territory where people live, their rights as residents of such territory, and the activities of the search engines carried out on that territory.

However, we know that the WP29 considers that 'the deindexation from the search engines' European extensions on the ground that users tend to access the search engine via their national extension cannot be deemed as a sufficient means',[115] in spite of its empirical and statistical effectiveness and its intrinsic coherence.

Presentation and consequences of the 'glocal' option

Both global, as regards domain names, yet localized via the use of the Internet user's IP address, hence 'glocal', this technical method of the right to be deindexed borrows several elements from time-tested judicial practices. As such, it is viewed as a satisfactory method to implement the RTBF by a number of authors such as Rivero: 'Between the overreaching territorial application to all domains and the application only to the EU domains, a more reasonable option remains. Geofiltering seems the most appropriate approach to allow for effective protection of privacy rights while respecting the territoriality principle.'[116]

Geoblocking: a debate with inverted battlefields?

Deemed 'insufficient' by the CNIL,[117] in other cases, geoblocking was well received by the courts and even imposed by them on service providers located outside of the EU. This was the case in the famous *Yahoo*! Auctions case. So, what is this technology worth? How to assess such a technology that is at times found insufficient by some and sufficient by others, disregarded by the CNIL, yet demanded by the courts?

To answer these questions, we must come back to the *Yahoo*! case. On 22 May 2000, ruling through an interim order, the Paris Civil Court ordered Yahoo! Inc. 'to take all measures that may dissuade and make it impossible to view on Yahoo.com the auctioning of Nazi objects and on any other website or service that constitutes praise for Nazism or disputes Nazi crimes'.[118] Within this framework, on 11 August 2000, a panel of international experts was appointed to describe, in particular, 'the filtering procedures that may be implemented by Yahoo! Inc. to prohibit access, by Internet users operating from French territory, to sections that could be deemed unlawful by French courts'.[119]

In their brief, which is set forth in the text of the order of 20 November 2000, the experts point out that the Internet protocol (IP) associates the sender's IP address to the recipient's IP address for each packet of information transmitted. The website consulted is, therefore, capable of knowing the IP address of the Internet user requesting information. In this case, in an estimated 70 per cent of cases, the IP address will be identified as having been attributed to a French access provider.

This figure of 70 per cent was calculated based on the information provided by the Professional Union of Internet service providers (AFA). In an estimated 20 per cent of cases, the IP address provided by the access provider does not allow one to determine the Internet user's geographic origin. This situation notably involves international access providers, such as AOL, or certain private networks of large companies.

In 2000, as no filtering technology allowed one to locate all French Internet users connected from French territory, the panel of experts then proposed to have Internet users provide an affidavit attesting to their nationality. This declaration would be provided when the Internet user first connected to the disputed website or in a search for Nazi objects.

As one author has observed,[120] 'another figure may be pointed to: 100% of Internet users who would like to

114 Ibid 3.

115 WP29 Guidelines (n 70).

116 See Á Fomperosa Rivero, 'Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality, European Union Law', Working Papers No 19, Stanford, Vienna Transatlantic Technology Law Forum, 44 <https://law.stanford.edu/publications/right-to-be-forgotten-in-the-european-court-of-justice-google-spain-case-the-right-balance-of-privacy-rights-procedure-and-extraterritoriality/>

117 CNIL's deliberation no 2016-054 (n 31).

118 Interim Order of 22 May 2000, *Yahoo v LICRA and UEJF*, Paris Civil Court.

119 Interim Order of 20 November 2000 (n 105).

120 V Sédallian, 'Commentaire de l'affaire Yahoo! (2), À propos de l'ordonnance du Tribunal de grande instance de Paris du 20 novembre 2000' [Commentary on the Yahoo! (2) Case, Regarding the Paris Civil Court's Order of 20 November 2000], Juriscom.net (24 October 2000) <http://lthoumyre.chez.com/chr/2/fr20010112.htm>

bypass the filtering are likely going to be able to do so. The order gives three means of bypassing this filtering: using AOL as access provider, going through an 'anonymization' service and using a browser in English.'

Despite the estimated rate of 70 per cent[121] and the risks of bypassing, as previously mentioned, the French court nevertheless maintained its initial decision. The Paris Civil Court considered 'that it has been demonstrated that it [Yahoo! Inc.] had the filtering technological and operational means'.[122] The court, therefore, implicitly considered that this geoblocking solution, with its imperfections and completed with other measures, was 'sufficient', given the objectives pursued and the useful effect of its decisions.

The comparison with the right to be deindexed is enlightening because, according to some figures, the geoblocking technology currently implemented by Google and Microsoft are more than 99 per cent effective.[123]Why was the court, the guarantor of individual freedoms pursuant to Article 66 of the French Constitution, satisfied with this measure, but the CNIL and the WP29 were not? This situation with inverted battlefields in a way is quite surprising. Indeed, in this case involving Yahoo! Inc., the American company, which was initially reluctant to implement any geoblocking measures, progressively rallied behind them, leading the court to be satisfied with them. On the other hand, in the case of the right to be deindexed, the geoblocking proposal was introduced at Google's initiative but deemed insufficient by the CNIL, which appears to be searching for an absolute, complete and technically perfect solution (See section 'Risk of 'bypassing': are the regulators in search of the ultimate solution?' below).

Geoblocking, a common practice in courts

In addition to the *Yahoo*! case, court practices show a number of decisions relying on geoblocking and, in particular, in the copyright field and/or involving libel on the Internet.

As regards copyright, within the framework of the special interlocutory injunction provided by Article L. 336-2 of the French Intellectual Property Code, the Paris Civil Court has handed down several particularly interesting decisions involving filtering and geoblocking.[124] In *The Pirate Bay* case, which involved access from France to a website for exchanging peer-to-peer music files, films, and video games, the court ordered the Internet access providers to 'implement all measures to prevent access *from French territory*'[125] (emphasis added) to the disputed websites.

The court's decision left each provider the freedom to determine the measures that permitted 'by any means and notably by blocking domain names'[126] access to the disputed websites from France for 12 months.

As regards the dispute involving libel on the Internet, once again, in several cases, the Paris Civil Court ordered the access providers to 'stop the harm' and to 'block or have the [disputed] website blocked',[127] with the access providers being required to implement all resources, 'they may have with the current state of their structure or of the technology (blocking by the IP or blocking by the DSN)'.[128] In another more recent case, the Paris Civil Court ordered the Internet access providers to implement all measures for preventing the access of their subscribers 'located in French territory' to the content of the disputed website, while leaving them the 'choice of the blocking measures, including with the IP or DNS'.[129] The maximum duration of these measures was once again also 12 months, but because this duration was deemed sufficient for a court to make a ruling on the merits of a claim filed in the lower court with third parties petitioning for indemnification (*partie civile*).

This quick detour through a selection of case law is of interest in illustrating the frequency, and, therefore, likelihood to be deemed effective by a court, of the filtering measures based on the IP address and targeting people living in French territory. One can legitimately ask the reasons for which, within the framework of the right to be deindexed, these measures have become insufficient.

Although, in its *Google Spain* judgment, the court wishes to guarantee 'effective and complete' protection for the right to be deindexed, the court must take into consideration the data subject's legitimate interests and the harm he may suffer due to the accessibility of the content he asks to be removed. But, since the purpose of the RTBF is to remedy this harm and not to compensate the damage incurred, the assessment of which will be subject to courts' discretionary powers, the deindexation measure ordered must be proportionate to such harm.

121 Which reached 90 per cent if it was completed with the Internet user's sworn affidavit, as the order states, 16.

122 Interim Order of 20 November 2000 (n 105).

123 Chabert (n 53) 4.

124 Paris Civil Court, Allostreaming case, 8 November 2013; Paris Civil Court, The Pirate Bay case, 4 December 2014; Paris Civil Court, T411.me case, 2 April 2015.

125 Paris Civil Court, *The Pirate Bay* case, 4 December 2014.

126 Ibid.

127 Paris Civil Court, Copwatchnord, interim order, 14 October 2011.

128 Ibid.

129 Paris Civil Court, Syndic Avenir, interim order, 20 October 2017.

This harm implies that there exists a form of a territorial attachment link between the data subject, his living environment, and the content whose deindexation is being requested. Indeed, invasion of privacy will be all the more likely since the disputed content will be visible and accessible in the data subject's country, by his friends and family and possibly by his employers, etc. Conversely, the fact that content is not deindexed for a user living completely on the other side of the world will probably not create any harm for the data subject.

Similarly, as regards the remedying of damage, courts use as a basis the existence 'of a sufficient, substantial or significant link' between the facts and the damage.[130] The CJEU has ruled that a criterion for jurisdiction for remedying all of the damage is the place where the person 'has his center of interests.'[131] The implementation of the RTBF could rely on these criteria, which have been established by the Court and national courts and give a protective, maximum legal effect to deindexation in the geographic area where the data subject 'has his centers of interest', including through geoblocking.

Risk of 'bypassing': are the regulators in search of the ultimate solution?

While recognizing that geoblocking represented 'progress', the CNIL, however, found it insufficient, which is the reason why Google Inc was fined. The CNIL's sanction committee found that 'the criterion of the IP's localization, which makes the protection granted to a European resident dependent upon the geographical localization such resident performs a search in the search engine, *is not, as a principle, satisfactory*'[132] (emphasis added). The CNIL added that 'the protection of a fundamental right cannot vary depending on the data's recipient'.[133] Therefore, this constitutes a 'precedent' in favour of fundamental European rights. This is what confers on it this universal, general, and absolute scope.

The principle expressed in this 'precedent' is corroborated by technical considerations, emphasizing the fact that geoblocking may be 'bypassed'. The CNIL explains that a French Internet user could still have access to the deindexed content in three different situations. First, 'on the occasion of a stay in the European Union by searching on a search engine's extension outside of the European Union from a Wi-fi connection or when travelling outside of the European Union'.[134] Secondly, where that user lives in 'the border areas of the territory, often benefiting from dual coverage by the French telephone network and by the foreign telephone network',[135] which would allow him 'to escape the filtering measure through the attribution of a foreign IP address although he is located in French territory'.[136] Thirdly, such user may use technological solutions that 'permit bypassing the filtering measure proposed by the company by allowing Internet users to choose the geographic origin of their address (use of a VPN, for example)'.[137]

The CNIL provides valid examples of means allowing bypassing. However, it is hard to imagine technologies that would be impossible to bypass. Even if such technologies existed, would it be desirable to implement them at all costs?

Here again, reading the case law is very instructive. In *The Pirate Bay* case cited above, the defendant companies, which were, in particular, access providers, pointed out the 'ease with which social networks distribute advice allowing their members to be informed on the means for bypassing the restrictive measures that may be ordered by a court, which risks making any decision of this nature ineffective',[138] attempting to convince the court not to order such measures.

The court did not follow this argument while recognizing that it is 'accurate that a part of Internet users may bypass any blocking measures'. The Paris Civil Court's motivation is particularly interesting for the case of deindexation we are concerned with. Indeed, firstly, the court ruled 'that it is not established that a large majority of Internet users . . . have a firm desire to participate in worldwide piracy and on a large scale', and, secondly, that the contemplated measures 'target a large number of users, who do not necessarily have the time and the skills to search for the bypass methods that specialists find and memorize'.[139]

Moreover, in its *Telekabel* judgment of 27 March 2014, the CJEU has stated that 'it is possible that a means of putting a complete end to the infringements of the intellectual property right does not exist or is not in practice achievable, as a result of which some measures taken might be capable of being circumvented in

130 Paris Court of Appeal, 4th chamber, 6 June 2007.

131 Case C-509/09 *eDate Advertising GmbH and Others v X and Société MGN Limited* ECLI:EU:C:2011:685.

132 CNIL's deliberation no 2016-054 (n 31).

133 Ibid.

134 Ibid.

135 Ibid.

136 Ibid.

137 By doing this, the CNIL provides the bypass instructions, like the Paris Civil Court did on its order in the Yahoo! case (as Sédallian observed regarding the Paris Civil Court's order in the Yahoo! case (n 120) para 32.

138 Paris Civil Court, *The Pirate Bay* case (n 125).

139 Ibid.

one way or another'.[140] But, it suffices that these measures have the effect of 'making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter that has been made available to them in breach of the intellectual property right'.[141]

In the *Pirate Bay* case, this is the reason why the French court found that the fact that 'it is impossible to ensure complete and perfect enforcement of decisions that may be made is not an obstacle to the decision to authorize measures preventing access to the websites participating in the distribution of infringements online'.[142]

By analogy, does a 'large majority' of French Internet users affected by the right to be deindexed have the desire or the opportunity to use a foreign Wi-fi connection when travelling to a border region, or they have the 'knowledge' allowing them to deliberately use a VPN to change their IP address in order to '*neutralize*' the geoblocking? There is good reason to doubt it. Furthermore, must the fact 'that it is impossible to ensure complete and perfect'[143] enforcement of the right to be deindexed lead to disregarding geoblocking as a sufficient measure, although it is nearly 99 per cent effective, as was previously stated?

In this respect, it should be noted that, in a case involving blocking websites encouraging terrorism,[144] the French Council of State itself has ruled that 'the fact that it would be technically possible, for some, to bypass the block or the deindexation of the websites with illegal content cannot lead to regarding these mechanisms as unsuitable to the objectives pursued'.[145] One may, therefore, wonder why the very same Council of State decided to submit this territorial questions to the CJEU when, in other circumstances, it has clearly endorsed a technical solution that may be circumvented. Maybe for the Council of State it is a way 'to make the CJEU face its responsibilities',[146] as suggests Professor Debet?

Conclusion

Through these preliminary questions submitted to it, the Court, somehow, will have to devise a solution in the now classic opposition between networks and territories, thereby continuing its court-made case law. Yet, these questions also involve a dual missed opportunity. The first is the lost opportunity of not having submitted to the Court the question of 'single processing operation', the structuring, logical element of the substantive and territorial universal claim of the right to be deindexed. This is because accepting the 'single processing operation' is an obstacle to the emergence of a solution distinguishing between the applicability of European law depending on the processing involved. Indeed, if the systematic indexation of the web by robots is processing separate from the displaying of results about a specific person, then it is possible to consider that European law applies only to the second but not to the first. In doing this, it would have been possible to construct a differentiated legal and technical response, localized but effective, to the right to be deindexed without the risk of destabilizing the very heart of search engine's activity by risking, for example, to prohibit them from collecting personal data.

The other lost opportunity is that of the risk of a costly decision for the effectiveness of protecting people's rights. Indeed, in the event, the Court chooses the strict 'regional' option, that of deindexing on the extension of only the data subject's country of origin, and this would lead to conferring on the right to be deindexed a substantially narrower scope than that currently conferred on it by geoblocking. Doing the best thing is at times the enemy of good—in legal matters also.

Of course, the Court may adopt yet a different solution than the three options submitted by the Council of State.[147] For instance, another conceivable legal option would be one (i) relying on blocking measures based on where the Internet user's IP address is deemed to be located within the EU and (ii) applying the delisting measure to all the relevant domain names of the European Member States but not to all the existing domain names. In doing so, the effectiveness of the right to suppression would be ensured without giving it an excessive, universal, and debatable reach.

doi:10.1093/idpl/ipy025

140 Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH et Wega Filmproduktionsgesellschaft mbH* ECLI:EU:C:2014:192, para 60.

141 Ibid, para 64.

142 Paris Civil Court, *The Pirate Bay* case (n 125).

143 Ibid.

144 Within the framework of the claim for annulment against French Decree 2015-125 of 5 February 2015, regarding the blocking of websites encouraging acts of terrorism or praising such acts.

145 French Council of State, 15 February 2016, no 389.140.

146 A Debet, 'Deréférencement: .fr ou .com, la CJUE devra trancher' [Deindexation: .fr or .com, the CJEU will have to decide], Communication Commerce Électronique (October 2017) no10, 37.

147 As the CJEU is free to reword the question submitted and may then provide an answer differing from what is precisely contained in the question (see, for instance, Case C-234/01 *Arnoud Gerritse contre Finanzamt Neukölln-Nord* ECLI:EU:C:2003:340).