The Right to Be Forgotten in the European Union

Miquel Peguera

1. Introduction

Among the huge volume of content that is made available at a rapidly growing pace on the internet, it is only natural that we find abundant information related to identifiable individuals. Such information may be inaccurate, may be shown out of context, may be decades old and have become embarrassing or damaging today. Even where it is perfectly accurate information, its current availability on the net—particularly when search engines cause such information to emerge as one of the first results in a search made on the basis of an individual's name—may harm in different ways the person to which it refers, distorting or ruining one's reputation. Even if it is not harming, the individual may not want such information to be permanently remembered and linked to him or her. He or she wants to escape from it, to be left alone—to 'be forgotten'.

The problem of the widespread availability of privacy-damaging information is not new. It has been dealt with since long before the internet era, sometimes under the label of *droit à l'oubli*, particularly in connection to mass media publications.[1] Nonetheless, the issue has grown to an unprecedent level after the irruption of the web, the digitization of press archives, and the easiness to find information thanks to search engines.[2]

The right to protection of personal data, enshrined as an autonomous right by the EU Charter of Fundamental Rights,[3] which is in some respects wider than that of privacy notwithstanding their overlaps,[4] has been seen as a particularly fitting tool to regain control over the dissemination of personal information on the internet. Indeed, data protection, as conceived in EU law, is essentially a right of informational self-determination.[5] It includes the right to have personal data erased wherever they are unlawfully processed—irrespective of whether such processing amounts to a violation

---

[1] See Alessandro Mantelero, 'The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'' (2013) 29 Computer L & Security Rev 229, and references therein.

[2] See eg Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the* Digital Age (Princeton U Press 2009).

[3] See Charter of Fundamental Rights of the European Union [2012] OJ C 326/391 (Charter), Art 8. On the recognition of data protection as a fundamental right, see Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

[4] See eg Orla Lynskey, 'Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order' (2014) 63 Int'l & Comparative L Quarterly 569.

[5] See Giancarlo Frosio, 'Right to Be Forgotten: Much Ado About Nothing' (2017) 15(2) Colorado Tech L J 307, 313.

of privacy—except where there is a competing right or interest that should prevail. The 1995 Data Protection Directive—now replaced by the General Data Protection Regulation (GDPR)[6]—already granted a right of erasure, so data subjects may obtain, 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]

When the works for revamping the EU data protection legal framework started around 2010, the EU Commission emphasised the need of strengthening data subjects' control over their data,[8] noting that the effective exercise of the rights provided for by the Directive was still challenging, especially regarding the online environment. Specifically, the Commission sought to 'clarifying the so-called 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.'[9] The label 'right to be forgotten' made its way to the final text of the GDPR, if only in brackets and in double quotes, in the title of Article 17, devoted to the right to erasure—somehow conveying that such a right encompasses a 'right to be forgotten.'[10]

Nonetheless, the GDPR did not expressly codify the outcome of the landmark 2014 ruling issued by the Court of Justice of the European Union (CJEU) in the *Google Spain* case.[11] The ruling held that internet search engines' are obliged to remove the search results pointing to personal information which is deemed to be 'inadequate, irrelevant or no longer relevant, or excessive,'[12] where the search is made on the basis of the data subject's name. Such a tailored right is commonly referred to as the 'right to be forgotten'—or the 'right go be delisted' from the search results. While not specifically reflected in the GDPR, the grounds the CJEU found in the Directive for recognizing such a right—i.e. the right to erasure and the right to object to the

[6] See Regulation 2016/679/EU 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 [2016] OJ L 119/1 (GDPR).

[7] See the no-longer-in-force 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 L 281/31, Art 12(b).

[8] See European Commission, 'A comprehensive approach on personal data protection in the European Union' (Communication) COM (2010) 609 final.

[9] ibid 8. See also the speech by Viviane Reding, Vice-President of the European Commission, responsible for Justice, Fundamental Rights and Citizenship at the European Data Protection and Privacy Conference, 'Privacy matters – Why the EU needs new personal data protection rules' (Brussels, 30 November 2010) <http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm>.

[10] However, there is little in Article 17 which was not already recognized to data subjects in the Directive, and thus it is not clear that the right to erasure has been enhanced meaningfully with the GDPR, the addition of the right-to-be-forgotten words being arguably cosmetic.

[11] See C-131/12 *Google Spain SL v. Agencia Española de Protección de Datos* [2014] ECLI:EU:C:2014:317 (*Google Spain*).

[12] *Google Spain* (n 11) para 94.

processing—are also present in the GDPR. Therefore, the CJEU's holdings in *Google Spain* must be deemed essentially applicable also under the GDPR.[13]

This chapter will briefly consider two manifestations of the right to be forgotten as they are being currently applied in the EU. First, the right to be forgotten vis-à-vis internet search engines, i.e., the right to be delisted from search results. Second, the right-to-be-forgotten claims directed against primary publishers to have the information deleted or anonymized at the source.

2. The Right to Be Forgotten Vis-À-Vis Search Engines

Under EU data protection law, the so-called right to be forgotten may be exercised by a data subject through the right of erasure—now also labelled as 'the right to be forgotten' in Article 17 of the GDPR—or via the right to object to the processing, where the conditions for any of those rights are met. Such claims may be directed to any data controller. In practice, however, the most relevant development of the right to be forgotten has consisted of its use *vis-à-vis* internet search engines, following the recognition of this right by the CJEU in *Google Spain*.

2.1. *Google Spain*

As a threshold question, the Court in *Google Spain* dealt with the territorial scope of the then-in-force Data Protection Directive. It found that it was applicable to the processing of data carried out outside the EU by a non-EU company—in the case, Google Inc. The Court found that the processing was carried out 'in the context of the activities of an establishment' of the search engine in Spain, even though such an establishment—Google's Spanish subsidiary—confined its activities to promote and sell advertisement space offered by the search engine.[14] As a result, one of the connecting factors provided for in the Directive to trigger its applicability was met.[15] The same conclusion may certainly be reached under the GDPR, as it provides—even more broadly—for the same connecting factor, and generally widens the territorial scope compared to the Directive.[16]

The Court also held that a search engine's operator (i) carries out a *processing* of the personal data included in the webpages it indexes and gives access to through the search results, a processing which is different from that carried out by the websites where the information is located;[17] and (ii) is a *data controller*, as it determines the

[13] However, Articles 17(3)(a) and 85 GDPR offer more room to take freedom of expression into account.

[14] See *Google Spain* (n 11) para 60.

[15] See Directive 95/46/EC (n 7) Art 4(1)(a).

[16] See GDPR (n 6) Art 3.

[17] *Google Spain* (n 11) para 35.

purposes of the means of such a processing.[18] Again, the basis for such conclusions may also be found in the GDPR's definitions of processing and controller.

After redrafting some of the questions posed by the national court so as to be able to give a somewhat narrow answer, the Court held that the right to erasure and the right to object—provided that their conditions are met—allow data subjects to require the removal of search results pointing to personal information in searches carried out on the basis of the data subject's name. Under the Directive, the right to erasure was granted where the processing of data does not comply with the provisions of the Directive—thus, for instance, where the data are inadequate, irrelevant or excessive in relation to the purposes of the processing, as that would entail not complying with the Directive's requirement of data quality.[19]

According to the CJEU, the data subject does not need to have suffered any prejudice;[20] the data does not have to be necessarily unlawful, inaccurate or untruthful, or even be private information. In addition, there is no need to have the content erased beforehand or simultaneously from the publisher's web page, nor even to ask the publisher for such a removal. The data subject may directly request the delisting of the search results to the search engine's, as it carries out a separate and additional processing from that carried out by the primary publisher.[21]

The CJEU made it clear that a fair balance should be sought between the legitimate interest of internet users in accessing the information and the data subject's fundamental rights under Articles 7 and 8 of the Charter. It held that, as a rule, data subject's rights will override those of internet users, though in some cases the outcome may depend '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.'[22]

---

[18] ibid para 33.

[19] See Directive 95/46/EC (n 7) Art 6(c). Similarly, the principle of data minimisation under the GDPR requires the data to be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (Article 5(1)(c) GDPR).

[20] *Google Spain* (n 11) para 96.

[21] ibid para 88.

[22] ibid para 81. Some criticism about the way the CJEU framed the balancing of rights can be seen, for instance, in Stefan Kulk and Frederik Zuiderveen Borgesius, '*Google Spain v. González*: Did the Court Forget About Freedom of Expression?' (2015) 3 Eur J of Risk Reg 389; Christopher Rees and Debbie Heywood, 'The 'Right to be Forgotten' or the 'Principle That Has Been Remembered'' (2014) 30 Computer L & Security Rev 574; Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc. v. Agencia Espanola de Proteccion de Datos*' (2014) 14 Human Rights L Rev 761; Michael Rustad and Sanna Kulevska, 'Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow' (2015) 28 Harv J L & Tech 349; Anna Bunn, 'The Curious Case of the Right to be Forgotten' (2015) 31 Computer L & Security Rev 336; Miquel Peguera, 'The Shaky Ground of the Right to Be Delisted' (2016) 18 Vanderbilt J of Entertainment & Tech L 507.

As a result, search engine operators must assess on a case-by-case basis the merits of the right-to-be-forgotten requests and make a decision taking into account the rights and interests involved.[23] When a request is rejected by the search engine, the data subject may resort to the Data Protection Authority (DPA), which may order the search engine to delist the link. Courts may also be involved, either where a data subject files a judicial complaint asking for the removal, or where the DPA's decision is appealed.

2.2. Delisting in Numbers

When considering the practical application of the right to be forgotten in relation to search engines results, Google is of course the crucial source of information to look at, not the least because of its absolute dominance in Europe, where it holds more than 90% of the market share for search engines.[24]

According to Google's transparency report,[25] from 29 May 2014—when it launched its official request process dealing with the right to be forgotten—up to the end of May 2019, it received 811,029 requests to delist. Each request may comprise one or more URLs to be delisted. The requests received in that period comprised 3,170,113 URLs. Out of all requests fully processed by Google as of 30 May 2019, the search engine delisted 1,218,113 URLs (44,6%) and rejected delisting 1,510,436 URLs (55,4%).[26]

Most of the requests (88,5%) come from private individuals. The remaining 11,5% are requests made by government officials, other public figures, minors, corporate entities and requests made on behalf of deceased persons.

Regarding the type of websites targeted, starting from 21 January 2016, when Google began recording this information, 16,3% of the URLs evaluated were hosted on directories or aggregators of information about individuals such as names and addresses, 11,6% on social networking sites, 18,7% on the website of a media outlet or tabloid, 2,4% on official government websites, and the rest on different sites fitting under a broad 'miscellaneous' category.

Concerning the kind of information—also from January 2016—it may be highlighted that 17,7% of URLs related to professional information. In addition to those, content related to professional wrongdoing made up 6,1% of URLs, and crime represented 6,2%. Pages containing self-authored content made up 6,8% of URLs.

---

[23] On the role of search engines in deciding about delisting requests, *see* Maria Tzanou, 'The Unexpected Consequences of the EU Right to Be Forgotten: Internet Search Engines as Fundamental Rights Adjudicators' in Christina Akrivopoulou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, forthcoming 2019).

[24] See Statcounter <http://gs.statcounter.com/search-engine-market-share/all/europe>.

[25] See (2019) <https://transparencyreport.google.com>. For a detailed research paper covering up to 31 December 2017, see Theo Bertram and others, 'Three years of the Right to be Forgotten' (2018) <https://g.co/research/rtbf_report>.

[26] Google, 'Transparency Report' (n 25). The number of URLs does not include those not fully processed as of 30 May 2019.

Non-sensitive personal information, such as addresses, contact details or other content represented 5,7%. In addition, many requests—comprising 25,7% of the URLs—did not provide sufficient information as to be located or evaluated. In other cases, the name of the requester did not appear on the webpage (14,7%).

URL delisting rate is 100% where the name is not found on the webpage—it must be recalled that delisting only implies that the result will not be shown in searches by the person's name, and the information may still be retrieved using other search queries. Conversely, requests that lack sufficient information are not delisted. A very high delisting rate applies to non-sensitive and sensitive personal information. Crime related content is delisted in less than half of the cases, as well as self-authored content. Professional information and content related to professional wrongdoing have a very low delisting rate; and even a lower rate applies to political information.

2.3. Balancing Rights

The balancing exercise required by the CJEU lies at the core of any delisting decision. Each search engine uses its own tools and criteria to make a decision about the requested removal. Some helpful criteria were provided by the Guidelines issued by the Article 29 Working Party (Article 29 WP).[27] A small fraction of data subjects who don't agree with the search engine's response bring the case before the DPA or before the courts. As a result, a body of case law is being created, which deals with a variety of situations and reflects the different cultural approaches to freedom of expression and information. By way of illustration, some cases will now be briefly considered—most of them from Spain, which is by far the EU country where more court rulings have been handed down regarding delisting requests.[28]

A relevant case in the UK is *NT1, NT2 v Google LLC*,[29] which decides on two separate claims by two data subjects, referred to in the ruling as NT1 and NT2. Both were businessmen who had been convicted of criminal offences long time ago. They requested Google to delist search results to information about their convictions. After Google rejected to delist most of the links they brought judicial proceedings seeking orders to remove the links as well as compensation from Google. Claimants alleged that the information was inaccurate and, in any event, out of date, not relevant, of no public interest, and an illegitimate interference with their rights. Interestingly, Justice Warby considered specifically the criteria contained in Article 29 WP Guidelines, finding particularly relevant the criterion regarding the cases where the data relate to

[27] See Art 29 Working Party (WP29), '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 González' C-131/12' (2014) 14/EN WP 225 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>.

[28] An overlook as of July 2015 is provided in Miquel Peguera, 'In the Aftermath of Google Spain: How the 'Right to Be Forgotten' is Being Shaped in Spain by Courts and the Data Protection Authority' (2015) 23 IJLIT 325.

[29] See *NT1, NT2 v Google LLC* [2018] EWHC 799 (QB) (UK).

a criminal offence. The Guidelines state that '[a]s a rule, DPAs are more likely to consider the de-listing of search results relating to relatively minor offences that happened a long time ago, whilst being less likely to consider the de-listing of results relating to more serious ones that happened more recently. However, these issues call for careful consideration and will be handled on a case-by-case basis'.[30]

NT1 had been convicted of conspiracy to account falsely with the purpose of evading tax. He was sentenced to four years' imprisonment and received a disqualification from acting as a company director. The Court of Appeals noted that he had been the principal actor in the false accounting conspiracy.[31] Justice Warby rejected the requested delisting. He underlined that the claimant played a limited role in public life, and the information was not inaccurate, related to his business life, not his personal life, and originally appeared in national media, being a foreseeable consequence of his criminal conduct. Justice Warby concluded that the information retains sufficient relevance today, even though, thanks to a change in the law, the conviction was spent. He highlighted that NT1 remains in business and 'the information serves the purpose of minimising the risk that he will continue to mislead, as he has in the past'.[32]

A different outcome was reached regarding the second claimant. NT2 had been convicted of phone tapping and computer hacking, of which he pleaded guilty. He was sentenced to six months' imprisonment. In this case, Justice Warby found that the information had become out of date and irrelevant and there was no sufficient legitimate interest of internet users in its continued availability. The judge noted that the claimant's past offending was of little, if any, relevance to assess his suitability to engage in business, there was no risk of repetition, and no need for anybody to be warned about it.[33]

In the field of medical activity, a Spanish court ruling of 11 May 2017 tackled harsh negative comments about the professional conduct of a renowned medical doctor.[34] The comments were published on a website in 2008. Google rejected the delisting request alleging public interest in finding the information. The DPA then ordered Google to remove the result. Google appealed to the *Audiencia Nacional* (AN)—the competent court for revising the DPA's decisions. The AN took into account the criteria provided by the Article 29 WP and concluded that the link should not be delisted. The comments were covered by freedom of expression, the claimant was still working as a doctor and the interest of his future patients should prevail. They are entitled to know about his former patients' experiences and opinions. However, in another case also concerning the professional activity of a medical doctor, decided just two months later by the same court—though with a different judge-rapporteur—the

[30] See WP29, 'Guidelines' (n 27) 20.

[31] See *NT1, NT2 v Google* (n 29) paras 68-76.

[32] ibid para 170.

[33] ibid para 223.

[34] AN judgment of 11 May 2017 ECLI:ES:AN:2017:2433.

DPA's delisting order was upheld.[35] In the latter case the court argued that the publication was more than 20 years old; the doctor, who specializes in gynecology and obstetrics, lacks public relevance or public notoriety in his professional field, and it he had not committed a crime but a negligence fault.

Somewhat similarly, in a decision by a Dutch court of first instance, a surgeon who had been disciplined for medical negligence was granted a delisting request.[36] The surgeon was included in a website containing an unofficial blacklist of doctors. The court found that the website might suggest that the surgeon was unfit to treat people, which was not supported by the disciplinary procedure. It held that the surgeon's interest of not being matched with such a result in any search on the basis of her name should prevail over the public's interest.

In another ruling,[37] the Spanish AN reversed the DPA delisting order arguing that the information—a blog post casting doubts about the professional conduct of a businessman, with comments from different people—is protected by freedom of expression, noting as well that there is a public interest in accessing the information. Interestingly, the Court referred to the GDPR—in *dictum*, as it was not yet applicable at the relevant time—to underline that Article 17 GDPR expressly considers freedom of expression as an exception to the right to erasure.

Other cases concern information about political activities. In a 2017 ruling which denied the delisting, the Spanish AN held that access to information about the names of the candidates in a political election is of public interest and is required by the principle of democratic transparency.[38] The ruling cited a 2007 judgement of the Spanish Constitutional Court where it was held that a person who participates as a candidate in a public election cannot invoke a data protection right to limit access to that information, and that such information must be public in a democratic society.[39]

A relevant factor in any analysis is whether the information relates to the professional or to the personal life of the data subject—in the former case, the

[35] See AN judgment of 13 July 2017 ECLI:ES:AN:2017:3257.

[36] See Rechtbank Amsterdam decision of 19 July 2018 ECLI:NL:RBAMS:2018:8606. See also Daniel Boffey 'Dutch surgeon wins landmark 'right to be forgotten' case' (*The Guardian*, 21 January 2019) <https://www.theguardian.com/technology/2019/jan/21/dutch-surgeon-wins-landmark-right-to-be-forgotten-case-google >.

[37] AN, judgment of 12 December 2018.

[38] See AN judgment of 19 June 2017 ECLI:ES:AN:2017:2562. More recently, in a similar case, the court held likewise, denying the requested delisting. See AN judgement of 27 November 2018 ECLI:ES:AN:2018:4712.

[39] Spanish Constitutional Court judgment 110/2007 [10 May 2007] ECLI:ES:TC:2007:110.

protection is much lower.[40] In many cases, the elapsed time is also a relevant factor in the overall assessment, even though a long period of time is not necessarily required.[41]

In yet another a Spanish case, in this occasion concerning Yahoo,[42] the data subject requested the delisting of results pointing to information about the Cali Cartel and about the data subject's links with the smuggling of goods in Colombia. After Yahoo rejected the request, the individual obtained a delisting order from the DPA. Yahoo brought an appeal arguing that the data subject plays a relevant role in public life and the information relates to his commercial activities and is of social significance. The AN held that one of the links should be delisted indeed as, in view of the documents proving the closing of the criminal investigation and of the time elapsed—more than 20 years from the publication of the news report, and more than 15 years from the closing of the case—the information was obsolete and no longer relevant. However, it denied the removal of the other two URLs, noting that they referred to much more recent publications, the data subject is a prestigious businessman, and thus a public figure, and the public interest should prevail.

All in all, the examples above reveal that where there may be a significant public interest, such in cases affecting professional activities or concerning public figures, a truly case-by-case approach is followed, reaching sometimes diverging outcomes which not always are straightforward in view of the limited context some rulings provide.

2.4. Geographical Scope

Google Spain did not specify the territorial scope of the delisting. It was not clear in the judgment whether delisting the link on the search engine's website under the domain name corresponding to the country were the search is carried out (for instance, *google.fr*, in the case of France) would be enough; or rather, the link should be delisted on all the EU domains; or even if, irrespective of the place from where the search was initiated, the link should be removed on any domain name used by the search engine, including the *.com* and the country codes of non-EU countries—that is, globally.[43]

---

[40] See eg AN judgment of 6 June 2017 ECLI:ES:AN:2017:3111. In a case concerning a legal adviser at the Parliament, where the information was not just a critique of her professional performance, but included data about her relatives, spouse, ideology and religious believes, the AN ordered the delisting. See AN judgement of 5 January 2018 ECLI:ES:AN:2018:136.

[41] For instance, the lapse of three years was highly relevant for granting the delisting in a case concerning news information about the data subject's participation in a public demonstration. See AN judgement of 25 July 2017 ECLI: ES:AN:2017:3260.

[42] See AN (Administrative Chamber) judgment of 8 November 2017 ECLI: ES:AN:2017:5118.

[43] See eg Frosio (n 5) 329; Brendan van Alsenoy and Marieke Koekkoek, 'Internet and Jurisdiction After *Google Spain*: The Extraterritorial Reach of the 'Right to be Delisted'' (2015) 5 Int'l Data Privacy L 105.

The latter option appears to be the one favoured by the Article 29 WP in its guidelines on the application of *Google Spain*.[44] The Article 29 WP emphasised that the judgment establishes an obligation of results, which must be implemented in such a way that guarantees the effective and complete protection of data subject's rights, and that EU law cannot be easily circumvented. In this regard, it put forward that 'limiting de-listing to EU domains […] cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.'[45]

The practical application of this criterion has not been homogeneous. In a 2015 case,[46] the Swedish DPA ordered Google to delist some results globally. On appeal, however, the Stockholm Administrative Court upheld the delisting only for searches made from Sweden, thus reversing the global reach of the DPA's decision. In this regard, the Court argued that a global delisting would imply going beyond the scope of application of the Directive and prejudice legal certainty.[47]

The geographical scope of the delisting was brought before the CJEU in *Google v CNIL*, a case still pending at the time of writing this chapter. The Advocate General (AG) Szpunar delivered his Opinion on 10 January 2019, recommending a 'European delisting'—i.e. that search engines delist the links on any of their domain names, but only for searches carried out in the EU.[48]

In this case, the French Data Protection Authority (*CNIL*), ordered Google to delist certain links globally—on all domain name extensions of the search engine. Google rejected and offered instead to use geoblocking techniques to remove the links whenever a search is carried out from an IP address deemed to be located in the EU, regardless of the domain name utilized by the internet user. This was not accepted by the CNIL, who fined Google. On appeal, the *Conseil d'État* referred the question to the CJEU. It asked, in essence, (i) whether a search engine is obliged to delist globally; (ii) if not, whether it is enough to delist on the domain name of the State in which the request was made, or more generally on all domains of EU countries; and (iii) whether, in addition to the latter obligation, the search engine must employ geoblocking tools to remove the results in any domain for searches deemed to be initiated in the EU country of the data subject, or more generally in any EU Member State.

---

[44] See WP29, 'Guidelines' (n 27) 20.

[45] ibid para 20. While it is true that the WP29 did not state that the delisting should be made on *all* domain names, but on the *relevant* ones, it certainly included the *.com* domain, which in any event is rejected by those opposing a global delisting.

[46] See Nedim Malovic, 'Swedish court holds that Google can be only ordered to undertake limited delisting in right to be forgotten cases' (*The IPkat*, March 2018) <http://ipkitten.blogspot.com/2018/05/swedish-court-holds-that-google-can-be.html>.

[47] ibid

[48] See C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:15, Opinion of AG Szpunar (AG Opinion in C-507/17).

AG Szpunar noted that the data subject's rights must be balanced against other fundamental rights, particularly that of receiving information, and that if worldwide delisting was to be imposed, EU authorities would not be able to define and determine a right to receive information, let alone to balance that right against other fundamental rights, particularly taking into account that the public interest of accessing information will vary from one third-country to another.[49] He warned against the risk of preventing people in a third-country to access the information. If the EU may impose a worldwide delisting, other countries may want to do the same according to their own laws, thus giving rise to a race-to-the-bottom, affecting freedom of expression both at the European level and globally.[50] As to the other questions, AG Szpunar underlay that *Google Spain* ordered the search engine to 'ensure, within the framework of its responsibilities, powers and capabilities,' that the processing meets the Directive, so that an 'effective and complete' protection of data subjects' rights is achieved.[51] He concluded that the delisting should therefore cover any search carried out from a location in the EU. The search engine operator should employ all means at its disposal to ensure that such a delisting is effective and complete, which includes resorting to geoblocking techniques.[52]

As noted, at the time of writing the CJEU has not decided on the case yet and thus the geographical scope of the delisting is still an open question, with different approaches followed by courts and DPAs.

2.5. Sensitive Data

Characterizing a search engine as a data controller raises the question of how a search engine could possibly comply with all controllers' legal duties regarding the incredibly huge amount of data it indexes. To be sure, *Google Spain* held search engines must ensure compliance with the data protection legal requirements 'within the framework of its responsibilities, powers and capabilities.'[53] This may be understood as an acknowledgement of the impossibility for a search engine to perform all such obligations, and as an effective limitation of its obligations in that respect. Nonetheless, the matter requires clarification, particularly in relation to the prohibition of processing of 'special categories' of data—such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and data on health and sexual life.[54]

---

[49] ibid para 60.

[50] ibid para 61. AG Szpunar did not rule out that there may be situations were worldwide delisting could be required but notes that there is no reason for that in the case at issue.

[51] *Google Spain* (n 11) para 38.

[52] See AG Opinion in C-507/17 (n 48) para 78.

[53] *Google Spain* (n 11) para 38.

[54] See Directive 95/46/EC (n 7) Art 8 and GDPR (n 6) Arts 9 and 10 GDPR. See also Joris van Hoboken, 'Case note, CJEU 13 May 2014, C-131/12 (Google Spain)' (2014) SSRN Research paper no 2495580 <https://ssrn.com/abstract=2495580>

This issue is tackled in another case referred to the CJEU by the *Conseil d'État*—still pending at the time of writing this chapter. The questions include how search engines should act when required to remove links to information containing sensitive data, and how the exception based on freedom of expression should play out in those cases. In his Opinion,[55] AG Szpunar suggested the Court to answer that the prohibition of processing sensitive data does apply to a search engine operator, but—following the language in *Google Spain*— only within the framework of its responsibilities, powers and capabilities, noting that an *ex ante* control by search engines would be neither possible nor desirable.[56] Crucially, AG Szpunar put forward that the Directive's prohibitions and restrictions regarding sensitive data cannot be applied to a search engine as if the search engine itself had put the data on the indexed webpages. Rather, they can only apply to a search engine by reason of the indexation and location of the information, and therefore, by means of an *ex post* verification after a delisting request.[57]

According to AG Szpunar, once the search engine, after a delisting request, ascertains the presence of sensitive data—except where it is covered by one of the exceptions to the prohibition—the removal should be systematic, without further assessment of competing rights and interests, as the prohibition of processing should not be deemed just one element to be considered among other factors.[58] If the processing by the webpage was illicit, so it must be considered the further processing by the search engine.[59] The AG noted that this is all the more so under the GDPR, which has maintained the prohibition and even enlarged the relevant categories of data.[60] Nonetheless, as the prohibition does not apply where the processing is covered by an exception, the search engine might deny the delisting in those cases.[61]

Regarding the exceptions or derogations necessary to protect freedom of expression, the AG put forward that not only the original webpage but also the search engine may enjoy the benefit of freedom of expression, notwithstanding *Google Spain*'s dictum apparently suggesting the opposite.[62] Thus, if the processing of sensitive data by the webpage was protected by freedom of expression, the search engine should also be able to deny the requested delisting—after a careful assessment of all the rights and interests involved.[63] He noted that, ultimately, freedom of

---

[55] See C-136/17 *G C, A F, B H, E D v Commission nationale de l'informatique et des libertés (CNIL)*, [2019] ECLI:EU:C:2019:14, Opinion of AG Szpunar (AG Opinion in C-136/17)

[56] ibid paras 49-54.

[57] ibid para 57.

[58] ibid paras 62-74.

[59] ibid para 72.

[60] ibid para 73.

[61] ibid para 77. It seems safe to understand that AG Szpunar is assuming that such a possibility would only be the case where the search engine concludes that there is a prevailing public interest in accessing the information, as in any other right to be forgotten request.

[62] ibid para 86.

[63] ibid paras 87, 92.

expression is one of the factors to be considered in the overall assessment of competing rights and interests by the search engine. Furthermore, the AG underlay that Article 17 GDPR, establishes that the right to be forgotten will not apply where the processing is necessary for exercising the right of freedom of expression and information.

This AG's conclusion seems in line with that of a Dutch case reported by Kulk and Borgesius.[64] There, the lower court ordered Google to delist a link to information about a criminal conviction, which under Dutch law is considered sensitive data, precisely because of the sensitive character of the data.[65] On appeal, however, the ruling was reversed, and the Court held that the search engine could benefit from the exception for journalistic purposes.[66]

3. The Right to Be Forgotten Vis-À-Vis Primary Publishers

While the right to be forgotten has most dramatically affected search engines, requests and legal actions have also been brought against primary publishers of the information. As *Google Spain* noted, the assessment of the competing rights and interests in those situations may be different than when referring to a search engine processing. Most cases refer to information appearing in newspapers' digital archives National courts have reached different results, and the ECtHR has had the occasion to balance the rights at stake.

There have been divergent rulings regarding claims seeking to anonymize newspapers' digital archives. The Belgium Supreme Court (*Cour de Cassation*) upheld in 2016 a lower court decision ordering *Le Soir* to anonymize the name of the claimant in the online version of an article published in 1994.[67] The article reported the conviction of the claimant, who caused a car accident, in which two people died, while driving under the effects of alcohol. The action was based on the claimant's right to be forgotten under the general right to privacy, rather than being a claim based on data protection. The court held that, in the circumstances of the case, after so many years from the initial publication, the claimant's right should prevail, hence the interference with the right to freedom of expression and information consisting in anonymizing the name of the claimant in the digital archive was justified.

Conversely, in a case against *El País*,[68] the Spanish Supreme Court, citing the ECtHR jurisprudence, denied in 2015 a claim to anonymize the newspaper's digital archive, as such archives are protected by the right to freedom of expression and information. The Court also rejected that the newspaper should delist the result in its

---

[64] Stefan Kulk and Frederik Borgesius, 'Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe' in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (CUP 2018)

[65] See Rechtbank Rotterdam decision of 29 March 2016 ECLI:NL:RBROT:2016:2395.

[66] See Hof Den Haag decision of 23 May 2017 ECLI:NL:GHDHA:2017:1360.

[67] See Cour de Cassation *Olivier G v Le Soir* [29 April 2016] no C.15.0052.F.

[68] See Supreme Court (Civil Chamber) judgment of 15 October 2015 ECLI:ES:TS:2015:4132.

website internal search tool.[69] The latter holding was nonetheless reversed by the Constitutional Court, holding that the claimant has the right to have the results delisted in the internal search tool—while upholding the conclusion that the archive should remain unaltered.[70] On a different note, the Supreme Court held in the same ruling that the publisher should have implemented exclusion protocols so that the content was not indexed by search engines. Failing to do so constituted an illegal processing by the publisher and thus the Court granted moral damages to the claimant. A similar measure mandating the use of exclusion protocols had already been held by the Hamburg Court of Appeal a few months earlier.[71]

Cases dealing with news publishers have also reached the European Court of Human Rights (ECtHR), which has engaged in balancing the competing rights and interests under the European Convention of Human Rights (ECHR). Namely, the right to respect for private and family life (Article 8) and the right to freedom of expression (Article 10), which encompasses the freedom to receive and impart information. The ECtHR jurisprudence confirms that Article 8 ECHR may serve as a basis for a right to be forgotten regarding primary publishers such as media organizations if, in an assessment of the relevant circumstances, the balancing of rights favours the individual's fundamental rights over the right to freedom of expression of the publisher and the public's right to receive information. Nonetheless, the ECtHR has stressed the important role of online archives' in preserving and facilitating public's access to news and information and has held that such archives fall within the scope of Article 10 ECHR.[72]

Indeed, the ECtHR has strongly protected freedom of information against attempts to supress information from press archives, even regarding information which was declared to be defamatory.

A case in point is *Węgrzynowski and Smolczewski v Poland*, concerning a newspaper article containing allegations of unlawful practices against the lawyers of some Polish politicians. A domestic court found the allegations to be unfounded and damaging to the lawyers' good name and reputation. Some years later, the plaintiffs discovered that the original article was still available on the newspaper's online archive and that it was highly positioned in Google's search results. They sought an order to remove the article from the online archive and compensation for non-pecuniary damages. The claim was rejected. The ECtHR underscored that the legitimate interest of the public in accessing the archive is protected under Article 10,[73]

---

[69] This was in line with the WP29 Guidelines, which noted that 'as a rule the right to delisting should not apply to search engines with a restricted field of action, particularly in the case of newspaper website search tools'. See WP29, 'Guidelines' (n 27) 8 (para 18).

[70]See Constitutional Court judgment of 4 June 2018 ECLI:ES:TC:2018:58.

[71] See Oberlandesgericht Hamburg decision of 7 July 2015 7U 29/12. See Irini Katsirea, 'Search Engines and Press Archives Between Memory and Oblivion' (2018) 24 European Public L 125.

[72] See *Times Newspapers Ltd (nos 1 and 2) v UK* Apps nos 3002/03 and 23676/03 (ECtHR, 10 March 2009) para 27.

[73] See *Węgrzynowski and Smolczewski v Poland* App no. 33846/07 (ECtHR, 16 July 2013) para 65.

and found no violation of Article 8. Agreeing with one domestic court, the ECtHR held that 'it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations.'[74]

When assessing the degree of the diffusion of a news report, the ECtHR considers the original reach of the publication, rather than the amplifying effects facilitated by search engines. In two cases where the Court tackled the applicants' contention that the content was readily available through search engines, the Court disregarded the claim noting that the applicants had not reached the search engine to have the links removed.[75]

In *M L and W W v Germany*, the ECtHR examined whether the German court's refusal to oblige media publishers to suppress from their news reports available online the names of two persons convicted of a murder in a famous case some years ago constituted a violation of those persons' right to private live.[76] The case concerned the murder of a popular actor, of which the applicants had been convicted and served time in prison. According to the German Federal Court, the concerned news reports were objective and truthful. Interestingly, in this case the ECtHR cited extensively the *Google Spain* judgment.

The ECtHR adopted the CJEU's reasoning noting that search engines' obligations regarding the affected person may be different than those of the publisher of the information. The Court stressed that while the initial publisher's activity lies at the core of what freedom of expression seeks to protect, the main interest of a search engine is not that of publishing the information about the affected individual, but to make it possible for the public to find the available information about that person and to establish a profile about him or her.[77]

The ECtHR jurisprudence provides for some criteria for weighing the interests at stake; namely the 'contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and, where it arises, the circumstances in which photographs were taken.'[78] Applying these criteria in *M L and W W v Germany*, the ECtHR found that the freedom of expression and information should prevail over the rights of the claimants, and thus that Germany did not incur in a violation of the latter. In particular, the ECtHR found that the news reports at issue did contribute to a debate of public interest. The issue at stake was not the initial publication of the news reports, but their availability years after the criminal procedure

[74] ibid

[75] See *Fuchsmann v Germany* App no 71233/13 (ECtHR, 19 October 2017) para 53; *M L and W W v Germany* Apps nos 60798/10 and 65599/10 (ECtHR, 28 June 2018) para 114.

[76] ibid

[77] ibid 97 (referring to *Google Spain*, paras 59-62).

[78] ibid 95.

had ended—when the data subjects were about to leave prison, and thus were all the more interested in no longer being confronted with their criminal past in view of their social reintegration. In this regard, the ECtHR fully agreed with the Federal Court in that the public has a legitimate interest not only in being informed about current events, but also in being able to search information about past events, and reminded that the public interest in accessing online press archives is protected under Article 10.[79] The ECtHR also warned that finding otherwise could give rise to a chilling effect, with news publishers avoiding making their archives available online or omitting parts of news reports.

In this case, the applicants did not intend to have the news reports deleted altogether, but only to have their names erased from them, which implies a lower degree of interference with freedom of expression. Nonetheless, the ECtHR held that including in a news report individualized elements such as the full name of the concerned person is for the journalists to decide—within the deontological rules of their profession—and that, in fact, including such details is an important aspect of the work of the press, all the more when it comes to reporting criminal proceedings that have aroused considerable public interest.[80]

4. Conclusion

The right to be forgotten is a broad category which refers to people's right to control the dissemination and persistent availability of information about them. The basis for such a right may be found in the fields of privacy, data protection and other personality rights. The most visible manifestation of the right to be forgotten focuses on obtaining the delisting from search results generated in searches by the name of the concerned person, and emerged in 2014, in the framework of data protection law, with the landmark CJEU's *Google Spain* judgment.

After almost five years since the *Google Spain* judgment, the right to be forgotten regarding search engines is well established and settled law. The key findings of the judgment, no matter how controversial they were at the time—and may still be—seem to have come to stay. Even more, as noted in the literature, the basic tenets of this right may be found also in other jurisdictions.[81] In any event, the delisting requests are routinely dealt with by search engines, DPAs and courts in Member States. While not incorporating the ruling in its precise details, the GDPR only enhances what the Court already devised based on the Directive—although arguably allowing for a better consideration of freedom of expression and information.

The key element when it comes to exercising the right is the appropriate balancing of rights and interests the search engine is called to perform in the first place. Search

[79] See *Węgrzynowski and Smolczewski* (n 73) para 65.

[80] See *M L and W W v Germany* (n 76) para 105. The ECtHR refers to *Fuchsmann* (n 75).

[81] See Krzysztof Garstka and David Erdos, 'Hiding in Plain Sight? The 'Right to Be Forgotten' and Search Engines in the Context of International Data Protection Frameworks' [2017] University of Cambridge Faculty of Law Research Paper No. 46/2017 <https://ssrn.com/abstract=3043870>.

engine's and DPAs seem to converge more and more in the criteria and results of the analysis, which in turn are modelled by court decisions. The areas where the outcomes are more unpredictable are those of information about professional performance, and of content related to crimes or to the involvement in actual or alleged unlawful activities in the past. Nonetheless, big open questions still surround the right to be forgotten. Two of them, extraterritoriality and sensitive data, have been highlighted in this chapter. At the time this book is published, however, they will most probably have been decided by the CJEU, in a sense which is difficult to predict.

The right to be forgotten is also being exercised against primary publishers, particularly in relation to press archives. Here the case law, led by the ECtHR jurisprudence, emphasises the importance of such archives for accessing information and tends to favour their inalterability, while accepting less intrusive measures to provide for some obscurity to benefit the individual expectations of oblivion.

REFERENCES

1. Alessandro Mantelero, 'The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'' (2013) 29 Computer L & Security Rev 229.
2. Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the* Digital Age (Princeton U Press 2009).
3. Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).
4. Orla Lynskey, 'Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order' (2014) 63 Int'l & Comparative L Quarterly 569.
5. Giancarlo Frosio, 'Right to Be Forgotten: Much Ado About Nothing' (2017) 15(2) Colorado Tech L J 307, 313.
6. Stefan Kulk and Frederik Zuiderveen Borgesius, '*Google Spain v. González*: Did the Court Forget About Freedom of Expression?' (2015) 3 Eur J of Risk Reg 389;
7. Christopher Rees and Debbie Heywood, 'The 'Right to be Forgotten' or the 'Principle That Has Been Remembered'' (2014) 30 Computer L & Security Rev 574.
8. Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc. v. Agencia Espanola de Proteccion de Datos*' (2014) 14 Human Rights L Rev 761.
9. Michael Rustad and Sanna Kulevska, 'Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow' (2015) 28 Harv J L & Tech 349.

10. Anna Bunn, ‘The Curious Case of the Right to be Forgotten’ (2015) 31 Computer L & Security Rev 336.
11. Miquel Peguera, ‘The Shaky Ground of the Right to Be Delisted’ (2016) 18 Vanderbilt J of Entertainment & Tech L 507.
12. Maria Tzanou, ‘The Unexpected Consequences of the EU Right to Be Forgotten: Internet Search Engines as Fundamental Rights Adjudicators’ in Christina Akrivopoulou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global, forthcoming 2019).
13. Miquel Peguera, ‘In the Aftermath of Google Spain: How the ‘Right to Be Forgotten’ is Being Shaped in Spain by Courts and the Data Protection Authority’ (2015) 23 IJLIT 325.
14. Brendan van Alsenoy and Marieke Koekkoek, ‘Internet and Jurisdiction After *Google Spain*: The Extraterritorial Reach of the ‘Right to be Delisted’’ (2015) 5 Int’l Data Privacy L 105.
15. Joris van Hoboken, ‘Case note, CJEU 13 May 2014, C-131/12 (Google Spain)’ (2014) SSRN Research paper no 2495580 <https://ssrn.com/abstract=2495580>
16. Stefan Kulk and Frederik Borgesius, ‘Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe’ in Evan Selinger, Jules Polonetsky and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (CUP 2018).
17. Irini Katsirea, ‘Search Engines and Press Archives Between Memory and Oblivion’ (2018) 24 European Public L 125.
18. Krzysztof Garstka and David Erdos, ‘Hiding in Plain Sight? The 'Right to Be Forgotten' and Search Engines in the Context of International Data Protection Frameworks’ [2017] University of Cambridge Faculty of Law Research Paper No. 46/2017 <https://ssrn.com/abstract=3043870>.