The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)

On 24 September 2019, the Court of Justice of the European Union issued two judgments further delineating the scope of the right to be forgotten in the context of search engines. In GC and Others (C-136/17), the Court decided that a search engine operator must only verify the lawfulness of its processing of sensitive data ex post, i.e. upon receiving a request for de-referencing. While lowering the level of protection of the right to data protection, this decision has to be understood as an act that brings the processing of sensitive data by search engines out of the grey area caused by the Court’s decision in Google Spain and Google (C-131/12) and into the sphere of legality. In Google v CNIL (C-507/17), the Court had to determine the territorial scope of the right to be forgotten. It established a general rule of EU-wide de-referencing in connection with measures preventing or at least seriously discouraging access to non-EU search results. This leaves space for non-EU States to find their own balance between data protection and freedom of information. Both decisions can be considered a balancing act of the Court in attempting to reconcile the often very diverging rights and interests of the involved subjects, this time mostly at the expense of the right to data protection.

I. Introduction

On 24 September 2019, the Court of Justice of the European Union (Court) issued two judgments pertaining to the so-called right to be forgotten. This right, which was established by the same court in May 2014 in its landmark decision in Google Spain and Google, is now enshrined in Art. 17 of the General Data Protection Regulation (GDPR). However, despite its codification, certain important aspects of the right to be forgotten remained unanswered. Both judgments complement the Court’s prior case-law in two crucial aspects. The judgment in Google v CNIL delineates the territorial scope of the right to be forgotten, whereas the case GC and Others addresses the processing of sensitive data by search engine operators and the de-referencing of such data – an area where interference with the data subject’s rights to privacy and protection of personal data is liable to be particularly serious due to the sensitivity of such data. In addition, the decisions provide further guidance on the relationship between the right to be forgotten and the freedom of information.

While according to Art. 17 GDPR the right to be forgotten (more correctly called the right to erasure) is a general right, it is of special importance in the context of search engines. Here, it is usually referred to as the right to de-referencing. Based on grounds relating to her particular situation, a data subject can request a search engine operator to remove (de-reference) from search results links leading to websites containing personal data pertaining to her, e.g. if the data are inadequate, irrelevant or no longer relevant in the light of the purposes for which they were collected and processed. It is important to note that this only holds true for searches conducted using her name, whereas such links can still be displayed if the search is conducted using other search terms. Furthermore, the display of a link in search results has to be considered separately from the initial publication of information. The data subject is not required to exercise her right to be forgotten with regard to both of them. Similarly, even if information is de-referenced from search results, it will still be visible on the webpage where it was initially published, save the data subject successfully invokes her right to erasure vis-à-vis the publisher of that webpage as well.

4 Case C-136/17 GC and Others EU:C:2019:773. See the text of the decision in this issue of GRUR International at DOI 10.1093/grurint/ikaa003.
5 ibid, para 67.
6 The presented basic principles pertaining to the right to be forgotten were established by the Court in its decision in Google Spain and Google. According to the art 29 Working Party, data processing by a search engine operator might become unlawful due the universal diffusion and accessibility of the information enabled by it, which might have disproportionate impact on privacy; Article 29 Working Party, 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 (WP 225) (2014) 6 <https://ec.europa.eu/justice/article-29/docs/40/document/opinion-recommendation/files/2014/wp225_en.pdf> accessed 2 December 2019.

© Published by DUP and CH Beck on behalf of GRUR e.V. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.
The right to be forgotten is an answer to an internet that ‘never forgets’, and can be understood as society’s capacity for forgiveness and empathy regarding past mistakes. It is based on the recognition that an individual has a significant interest in not being confronted by others with data from the past that are not relevant for current decisions and views about her. A very similar principle is established e.g. with regard to criminal records, where the records are deleted after a certain number of years. However, the right to be forgotten is not an absolute right: as the de-referencing of search results might negatively affect others, e.g. internet users trying to obtain information on a past event, such requests have to be carefully weighed against the latter’s freedom of information.

Although the referring court raised questions as to the interpretation of the Data Protection Directive (DPD), which is applicable in the proceedings before the referring court, the Court nonetheless also assessed the questions referred in the light of the GDPR ‘in order to ensure that its answers will in any event be of use to the referring court’. This is an unusual step as the aim of preliminary rulings according to settled case-law is not to enable the court to deliver advisory opinions, but rather to provide the guidance necessary for the effective resolution of a dispute at hand. Nonetheless, it is to be welcomed that by doing so, the Court cleared away doubts as to the transferability of its conclusions to the new legal regime.

II. Facts of the cases

In GC and Others, four applicants independently requested Google to de-reference various links to third-party websites containing sensitive data pertaining to them. The search results included a satirical photomontage of a former politician, an article naming an applicant as public relations officer of the Church of Scientology, an article concerning a judicial investigation relating to an applicant and reports on a criminal hearing during which an applicant was found guilty of sexual assaults on children. As the requests were rejected by Google, the applicants brought complaints before the Commission Nationale de l’Informatique et des Libertés (CNIL), the French data protection authority, which refused to serve formal notice on Google to carry out the de-referencing requested. Thereupon, the applicants made applications to the Council of State (Conseil d’État), which stayed the proceedings and referred to the Court questions relating to the applicability of the prohibition of the processing of sensitive data in the context of search engines and to the de-referencing of such data.

In the second case decided on the same day, Google v CNIL, the CNIL served formal notice on Google, demanding the latter to de-reference links from the search results globally, i.e. on all domain name extensions of its search engine. Google refused and confined itself to removing the links in question merely from the domain names corresponding to the versions of its search engine in the EU Member States, but it suggested complementing this solution with geo-blocking. This would prevent internet users with an IP address deemed to be located in the EU from accessing the affected search results, regardless of which version of the search engine they use (e.g. the Australian or the US-American one). The CNIL still considered this insufficient and thus imposed on Google a penalty of EUR 100,000. Google lodged an application with the Council of State aiming to annul the decision of the CNIL. The Council of State decided to stay the proceedings and referred to the Court questions as to the territorial scope of the right to be forgotten. Following the bringing of the request for a preliminary ruling, Google changed the layout of its search engine so as to automatically direct the internet user to the national version corresponding to the place where she is presumed to be conducting her search, regardless of which domain name she enters into the browser.

III. Applicability of the GDPR

In Google v CNIL, the Court first dealt with the territorial applicability of the GDPR. According to Art. 4(1)(a) GDPR, which corresponds to Art. 3(1) GDPR, the EU data protection law was applicable to data processing carried out in the context of the activities of an establishment of the controller on the territory of the EU. In Google Spain and Google, the Court interpreted this provision very broadly. Even though for the purposes of conducting a search, data was processed by the mother company located in a third state (namely Google Inc., with its seat in the United States of America) while the Spanish local branch only promoted the search engine and sold advertising space, the Court saw an inextricable link between both activities. Namely, it is the advertising activity of the local branch that renders the search engine profitable. On this basis, the Court concluded that data is processed in the context of the activities of Google’s Spanish subsidary, hence establishing the applicability of the DPD. Such an extensive interpretation of Art. 4(1)(a) DPD was due to the fact that the DPD did not provide for any other suitable rule establishing its applicability. Hence, if interpreted more restrictively, the processing of personal data of data subjects located in the EU by Google Inc. for the purposes of its search engine would fall outside the scope of the DPD – an outcome hardly compatible with the goals of EU data protection law.

Against this backdrop, the GDPR introduced in its Art. 3(2)(a) the so-called effects doctrine (Markortprinzip). The applicability of the GDPR was
expanded to the processing of personal data of data subjects located in the EU by a controller not established in the EU if the processing activities were related to the offering of goods or services to such data subjects, irrespective of whether a payment of the data subject was required. It was widely expected that the Court would now narrow its understanding of Art. 3(1) GDPR, and in future comparable cases rather rely on Art. 3(2)(a) GDPR. Nonetheless, the Court abode by its interpretation of Art. 3(1) GDPR. Therefore, the above-described principles established in Google Spain and Google remain valid under the GDPR.

Against the backdrop that Art. 3(2)(a) GDPR was introduced with the aim to accommodate cases like the one at hand, it is unclear why the Court did not revisit its interpretation of Art. 3(1) GDPR. Insisting on the old interpretation might lead to situations in which in some Member States the applicability of the GDPR will be established according to Art. 3(1) GDPR, whereas in other Member States the GDPR will be applicable, mutatis mutandis, to the same situations pursuant to Art. 3(2)(a) GDPR. This is due to the fact that the GDPR is only applicable under Art. 3(1) GDPR if data is processed in the context of the activities of an establishment of a controller in the EU. If, for instance, the search engine operator processed the data of internet users located in one of the smaller EU Member States in which it neither has an establishment nor in any way advertises its services, such link to activities of an establishment of the controller in the EU might not exist. The same would hold true if, in a specific Member State, the search engine operator advertised its services through a subsidy established in a third state rather than in an EU Member State. In such cases, the applicability of the GDPR will have to be established pursuant to Art. 3(2)(a) GDPR in order to guarantee the protection of the right to data protection throughout the EU.

IV. Processing of sensitive data by a search engine operator, and its de-referencing

1. Legal grounds for sensitive data processing by a search engine operator

a) General prohibition of processing of sensitive data

The GDPR governs the processing of so-called sensitive data in its Art. 9. As such data enjoy special protection, it is generally prohibited to process them. This is only lawful if one of the exceptions enshrined in Art. 9(2) GDPR is fulfilled. The latter are more restrictive than the legal grounds for the processing of ‘normal’ personal data in Art. 6 GDPR and only partially correspond to them.

Against this backdrop, Advocate General Jääskinen argued in Google Spain and Google against classifying search engine operators as controllers, arguing that an opposite decision, i.e. classifying them as controllers, would entail the processing of sensitive data by search engine operators incompatible with EU law. The Court nonetheless decided that a search engine operator is a controller, arguing that the processing of personal data by a search engine can be distinguished from, and is additional to, that carried out by the publishers of the websites listed in the search results. However, as in Google Spain and Google, the Court only dealt with the processing of ‘normal’ personal data, where the search engine operator can base data processing on its legitimate interests (Art. 6(1)(f) GDPR), the question as to what happens when sensitive data are processed remained unanswered. Numerous authors assumed that such activities are at least partially illegal. According to Advocate General Szpunar in GC and Others, a literal interpretation of the GDPR would indeed lead to this conclusion. It was therefore up to the Court to find a middle way, with a fair balance between the right to data protection on the one hand and the protection of the search engine operator’s business model and of the freedom of information of search engine users on the other.

The starting point of the Court’s assessment was its finding in Google Spain and Google that the search engine operator must ensure, within the framework of its responsibilities, powers and capabilities, that its activities meet the requirements set forth in data protection law. As the GDPR does not provide for a general derogation from the application of Art. 9 GDPR on the processing of sensitive data by a search engine operator, and as such an exclusion would run counter to the purpose of the provision (i.e. to ensure enhanced protection of sensitive data), the prohibition and restrictions laid down in Art. 9 GDPR apply also to search engine operators. However, the specific features of search engines and their limited capacity to decide which data are to be processed by them may have an effect on the extent of the operator’s responsibilities, powers and capabilities.

23 Pursuant to art. 4(7) GDPR, a controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of data processing. The controller is also responsible for the compliance with the GDPR.

24 Case C-131/12 Google Spain and Google EU:C:2011:424 = GRUR Int 2014, 719, Opinion of AG Jaaskinen, para 90.

25 Case C-131/12 Google Spain and Google EU:C:2014:317 = GRUR Int 2014, 719, paras 35-41.

26 Stefan Kulk and Frederik Zanderven Borgesius, ‘Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe’ in Jules Polonetsky, Omer Tene and Evan Selinger (eds), Cambridge Handbook of Consumer Privacy (Cambridge University Press 2017) 29 <https://sur.nim/abstract–2923722> accessed 2 December 2019; Yann Padova, ‘Is the right to be forgotten a universal, regional, or “glocal” right’? International Data Privacy Law 15, 17 (2019). Cf also Fiona Campbell, Data Scraping – What are the Privacy Implications? (2019) 20 Privacy and Data Protection 3, 4.

27 Case C-136/17 GC and Others EU:C:2019:14, Opinion of AG Szpunar, paras 45, 46.

28 Case C-136/17 GC and Others EU:C:2019:773, para 37, citing Case C-131/12 Google Spain and Google EU:C:2014:317 = GRUR Int 2014, 719, para 38.

29 Case C-136/17 GC and Others EU:C:2019:773, para 44.

30 ibid, paras 41-44.
users in Germany have to take down ‘obviously illegal content’ within 35 minutes. Not having actual knowledge of illegal activity or information, and that it is not unknown to the information society services for the information stored at the prohibitions and restrictions of Art. 9 GDPR cannot apply to a search engine operator ex ante and systemically, but rather by way of an ex post verification of the processing, under the supervision of the competent national authorities, on the basis of a request by a data subject. By deciding for an ex post control of the legality of processing of sensitive data, the Court de facto created an exception which is, according to the wording of the judgment, only applicable to search engine operators. With this exception, the Court brought search engine operators out of the grey zone in which the Google Spain and Google decision had left them and into the sphere of legality. In the light of the importance of search engines, and of Google’s search engine in particular, for the freedom of information of internet users within the EU, the Court rightly did not want to generally prohibit such processing. However, by doing so, the Court lowered the overall protection of sensitive data: as long as a data subject does not request that sensitive data pertaining to her be de-referenced, the search engine operator can lawfully process such data, even if no exception under Art. 9(2) GDPR is applicable. Unlike in other cases of data processing, data subjects hence have to make an effort to have their interests protected.

The decision de facto created a ‘notice and takedown’ procedure in the realm of Art. 9 GDPR. This is a mechanism not unknown to social platforms and other internet intermediaries. For example, it is enshrined in the eCommerce Directive and in the German Netzwerkdurchsetzungsgesetz (Network Enforcement Law). Still, unlike the latter regimes, where the ‘notice and takedown’ procedure relates to actions conducted by others (e.g. publishing of illegal content by a user of a social network), the ‘notice and takedown’ procedure under Art. 9 GDPR relates to actions (i.e. data processing) conducted by the company itself.

It remains to be seen whether companies from other business sectors will try to expand this exception to their respective fields. It seems that at least companies offering services based on web crawling are in a situation comparable to that of search engine operators, as they too search for information on the web without being able to ascertain in advance what data they will eventually ‘find’. On the other hand, the transferability of the exception to the processing of ‘normal’ personal data is of lesser importance, as in that case, data controllers are often able to process data based on their legitimate interests anyhow (Art. 6(1)(f) GDPR).

b) Exceptions allowing the processing of sensitive data

In the next step, the Court turned to the exceptions to the prohibition of sensitive data processing, which are enshrined in Art. 9(2) GDPR. Search engine operators could possibly invoke three of them, but must fulfil at least one to make data processing lawful. While it is hardly conceivable that a search engine operator could seek explicit consent (Art. 9(1)(a) GDPR) of data subjects affected by its referencing activities, the operator could also invoke Art. 9(2)(c) GDPR, which permits the processing of sensitive data manifestly made public by the data subject. Unfortunately, the Court did not provide any guidance on the interpretation of the notion ‘manifestly made public’. In any case, this exception might only be applicable to a very small fraction of sensitive data published online, as very often, sensitive data will not be published by the data subject herself but by somebody else, e.g. by a journalist, a friend or a coworker of the data subject. Apart from where the data subject has given consent to the processing of data or where data was manifestly made public by her, the operator could also base the processing on Art. 9(2)(g) GDPR if it is necessary for reasons of a substantial public interest on the basis of EU or Member State law. The Court identified such a substantial public interest in the right of freedom of information of internet users potentially interested in accessing relevant webpages, which is protected by Art. 11 of the Charter of Fundamental Rights of the European Union (Charter). Whether it will outweigh the data subject’s right to data protection has to be established in a balancing test. The factors to be taken into account in such a test correspond to the ones already established in Google Spain and Google, namely the nature of the information in question and its sensitivity for the data subject’s private life on the one hand, and the interest of the public in obtaining that information on the other. The interest of the public depends in particular on the role the data subject played in public life. As a general rule, the data subject’s rights will take precedence not only over the freedom of information of internet users but also over the economic interest of the search engine operator.

---

31 ibid, para 45.
32 ibid, para 47.
33 This was also observed by the German Bundesverfassungsgericht (Federal Constitutional Court) in its decision in Recht auf Vergessen II, cf Bundesverfassungsgericht, 6 November 2019, Recht auf Vergessen II, 1 BvR 276/17 para 113.
34 Art. 14(1) of the eCommerce Directive provides for an exemption from liability of information society services for the information stored at the request of a recipient of the service, provided that the provider does not have actual knowledge of illegal activity or information, and that it establishes a notice and takedown procedure; Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178/1.
35 According to §§ 1, 3 of the Network Enforcement Law (RGBl. I 3352), social networks with more than two million registered users in Germany have to take down ‘obviously illegal content’ within 24 hours after notification, whereas ‘illegal content’ has to be removed within seven days after notification.
36 Case C-136/17 GC and Others EU:C:2019:773, para 62.
37 ibid, paras 63, 64.
38 For example, friends and colleagues could publish sensitive data regarding a data subject on social networks or blogs, as in Case C-101/01 Lindqvist [2003] 1-12971.
39 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
40 Case C-136/17 GC and Others EU:C:2019:773, para 66. In his Opinion, AG Sepannr regretted that in Google Spain and Google the Court failed to bring more clarity by explicitly stating that in the framework of the balancing test, the freedom of expression of initial publishers of information, protected by art 11 of the Charter, also has to be taken into account; Case C-136/17 GC and Others EU:C:2019:14, Opinion of AG Sepannr, paras 68, 89, 92. Similarly, in its recent decision in Recht und Vergessen I, the German Bundesverfassungsgericht took the freedom of information of the initial publisher of information into consideration; cf Bundesverfassungsgericht, 6 November 2019, Recht auf Vergessen I, 1 BvR 1613, paras 110-111.
41 Case C-136/17 GC and Others EU:C:2019:773, paras 53, 66, citing Case C-131/12 Google Spain and Google EU:C:2014:317 = GRUR Int 2014, 719, paras 81, 99. On the contrary, the start point of the assessment of the German Bundesverfassungsgericht is that the right to data

4
Even though the exception enshrined in Art. 9(2)(g) GDPR might be most relevant for texts of a journalistic nature, it is not limited to them, as according to the Court, the balancing test has to be conducted in any event. More importantly, such balancing has to be conducted even if data processing does not correspond to the conditions of lawfulness and the restrictions set forth by the GDPR. It follows that even if no legal ground for data processing applies and/or the principles of data processing set forth in Art. 5 GDPR are not respected, the processing would still be lawful if the freedom of information of internet users overrode the rights and interests of the data subject.

In practice, the balancing test of Art. 9(2)(g) GDPR might only seldom have such a ‘healing effect’ on the processing of sensitive data without a legal basis or contrary to elementary data protection principles. In the case that data processing is lawful, the Court has held that the right to data protection usually overrides the freedom of information of internet users. This should hold all the more true if data are processed contrary to the elementary data protection principles. However, regardless of how often it will be invoked, this interpretation is a substantial development in the existing legal regime with a general character. Namely, as the Court did not restrict its statements to search engines, it is well conceivable that other data controllers processing publicly available data could also make use of this exception, especially if sensitive data are processed in the framework of journalistic activities. Thereby, and taking the very limited character of other exceptions of Art. 9(2) GDPR into account, the Court made Art. 9(2)(g) GDPR a central provision with regard to the processing of sensitive data.

2. De-referencing of sensitive data

According to the above-presented legal regime, a search engine operator is only obliged to assess the legality of the processing of sensitive data upon a request by a data subject. This will usually happen in the course of exercising one’s right to be forgotten according to Art. 17 GDPR.

When assessing whether a certain piece of information is to be de-referenced from search results, the data controller has to conduct a three-step test. First, the controller has to assess whether data is sensitive in the meaning of Art. 9(1) GDPR. If this is the case, the controller must in principle accede to the request for de-referencing. Second, the controller has to ascertain whether any exception of Art. 9(2) GDPR applies. If this is the case, and if all other conditions of lawfulness of data processing are fulfilled, the data controller may refuse the de-referencing request. However, it will still have to de-reference the links if the data subject has the right under Art. 17(a)(c) GDPR to object to that processing on compelling legitimate grounds relating to her particular situation, which must be assessed on a case-by-case basis. Lastly, and in any case, the data processor must ascertain based on Art. 9(2)(g) GDPR whether the inclusion of the link in search results is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that webpage by means of such a search.

This regime leans on the regime for ‘normal’ personal data and thus comes as no surprise. Of special interest is the third step of assessment pertaining to Art. 9(2)(g) GDPR. First, as stated above, it is surprising that Art. 9(2)(g) GDPR can ‘heal’ data processing not compliant with the principles set forth in the GDPR. So far, no comparable general exception exists for the processing of ‘normal’ personal data. Second, it is not entirely clear why, in the context of the right to be forgotten, the Court decided to conduct the balancing test in the framework of Art. 9(2)(g) GDPR rather than under Art. 17(3)(a) GDPR, which precludes the application of the right to be forgotten to the extent that processing is necessary for exercising the right of freedom of expression and information. At the stage of exercising the right to be forgotten, the balancing exercise would be better placed within Art. 17(3)(a) GDPR, which relates specifically to the right to be forgotten, whereas Art. 9(2)(g) GDPR relates to a different subject-matter, namely the lawfulness of sensitive data processing.

3. Duty of search engines to make a ‘correct impression’?

When answering a preliminary question regarding the de-referencing of data relating to a criminal procedure, the Court made a very interesting obiter dictum. It stated that in any event, i.e. even if a request for de-referencing is not granted, the search engine operator is required to adjust the list of results in a way that the overall picture it gives internet users reflects the current legal position. Practically, this means that links to webpages containing information on the current position must appear in the first place on the list. The search engine operator is obliged to comply with this rule in any event and at the latest on the occasion of the request for de-referencing.

While it is hard to disagree with the goal that the search results should reflect the true situation as much as possible, the Court has not stated on which provision this obligation is based. While protecting data recipients from false impressions and wrong conclusions is not one of the aims of data protection law, the Court could have been referring to the principle of data accuracy, enshrined in Art. 5(1)(d) GDPR. It stipulates that data shall be accurate and, where necessary, kept up to date, and that reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for

---

46 Case C-136/17 GC and Others EU:C:2019:773, para 69. In this context, the Court referred to the case-law of the European Court of Human Rights, which acknowledged that the public has an interest not only in being informed about a topical event but also in being able to conduct research into past events (M.L. and W.W. v Germany (2018) ECHR 354); ibid, para 76.
47 ibid, para 78.
48 Golland (n 44) 263.
49 ibid, 264.
which they are processed, are erased or rectified without delay. It seems that the Court considered search results to be one entity which, as a whole, must comply with Art. 5(1)(d) GDPR. This poses new questions, for example, who is competent to decide whether the ‘overall picture’ is correct, and what is the search engine operator obliged to do if no links reflecting the current position that could be displayed in search results exist? This could happen if the person is not in the limelight anymore, e.g. because she ceased to hold a political office.

The practical impact of this obiter dictum is yet to be seen. While the Court made this statement in the framework of a question dealing with the processing of data pertaining to offences and criminal convictions, and while it explicitly stated that the overall picture must reflect the current legal position, some authors seem to consider this rule to be generally applicable to any search result. In any case, as simply sorting search results in chronological order might not always suffice to leave a ‘correct impression’, this rule presupposes that the search engine understands the content of the data listed in the search results. This will require additional inputs on the side of search engine operators in the form of workers and/or algorithms sorting search results in such a way as to create a correct overall picture, and might set an end to the usage of algorithms that sort search results based on the (perceived) relevance for the internet user. This could create considerable challenges for search engine operators and possibly even affect the core of their business models. Furthermore, it is also questionable whether other data controllers, such as news publishers, are bound by the obligation to make a correct impression with internal on-site search results as well.

V. Territorial scope of the right to be forgotten

In Google v CNIL, the French Conseil d’État (Council of State) asked the Court for guidance on the territorial scope of de-referencing. Three options were identified: global de-referencing, i.e. de-referencing on all language versions of the search engine, EU-wide de-referencing and de-referencing merely on the language version of the search engine corresponding to the Member State in which the request for de-referencing was made, potentially in connection with the geo-blocking of search results on other language versions of the search engine.

The Court first noted that in a globalised world, even access to the information referenced in search results by an internet user located outside the EU is likely to have immediate and substantial effects on the affected person within the EU. Further, it referred to the goal of the EU data protection law, which is to guarantee a high level of protection throughout the EU, which can only be met in full by way of global de-referencing. Against this background, the Court explicitly confirmed the competence of the EU legislature to oblige search engine operators to de-reference search results on a global scale.

Interestingly, the Court continued by taking a step back. Taking into account that numerous third states do not recognise a right to be forgotten, and that it is in no way apparent from the wording of the GDPR that the EU legislature wanted to confer the right to be forgotten a scope going beyond EU borders, the Court came to the conclusion that currently, there is no obligation under EU law to carry out de-referencing on all language versions of a search engine. The Court rather opted for EU-wide de-referencing. As to different levels of protection of journalistic, artistic and literary expression among the EU Member States, which might influence the result of the balancing test, the Court referred to the cooperation mechanisms and instruments provided for by the GDPR. Using these instruments, it is for the data protection authorities to reach consensus and a single decision binding upon all of them.

In addition to EU-wide de-referencing, the search engine operator has to adopt, if necessary, sufficiently effective means capable of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question. Unfortunately, the Court did not further elaborate on when such measures are to be regarded as ‘sufficiently effective’. Despite being asked about the usage of geo-blocking technologies, it decided for a technology-neutral notion of preventive measures and left it for the referring Court to decide whether geo-blocking meets the requirements set forth by the Court.

Geo-blocking would locate, based on the IP address of the internet user, the current position of the internet user and block EU residents’ access to information on non-EU search domains. Although it can be circumvented, e.g. through a proxy or by using a virtual private network (VPN), which attributes an internet user an IP address belonging to another state, geo-localization can, as a rule, be deemed as effective enough to seriously discourage internet users in the Member States from gaining access to the links in question.
The Court stated that such preventive measures only have to be taken ‘if necessary’. Nonetheless, it is hardly imaginable how EU-wide de-referencing could be deemed effective if not accompanied by such measures. Therefore, such preventive measures will, as a general rule, have to be taken.

The decision of the Court for merely EU-wide de-referencing can be criticised.66 Namely, the GDPR regulates the relationship between a data subject and a controller with regard to the processing of data pertaining to that data subject, without making a distinction as to where the data is processed or who and where (the possible) recipients of the data are.68 In this regard, the Court argued that it is in no way apparent that the EU legislature would have conferred the rights enshrined in the GDPR a scope going beyond the territory of the EU Member States.69 This argument is not convincing. A glance into the provisions governing the territorial applicability of the GDPR reveals that the GDPR does have extraterritorial effects.70 This is most clear from Art. 3(2) GDPR. For example, according to Art. 3(2)(b) GDPR, the GDPR applies to the monitoring of users’ behaviour taking place in the EU (most often by setting cookies) even if the controller is not established in the EU. This leads to a de facto worldwide application of the GDPR, which has been criticised as ‘data imperialism’.71 Furthermore, it is not evident that any other provision would try to limit this broad scope of application of the GDPR. Lastly, the decision to differentiate processing activities based on national versions of a search engine is in a certain contradiction to the finding of the Court that Google is carrying out a single act of personal data processing.72 This speaks in favour of a single decision for all language versions.73

is more than 99 per cent effective. Dissenting Giorgia Bevilacqua, ‘The Territorial Scope of the Right to Be Forgotten Online in the Opinion of the Advocate General on the Case Google CNIL’ (2019) European Papers, vol 4, 2019, No 2, 656 <https://www.europeanpapers.eu/en/supplement/pdf_version/EP_EF_2019_H_004_Giorgia_Bevilacqua_2.pdf> accessed 4 January 2020.

67 In an assessment of the judgment in Google Spain and Google, art 29 Working Party also stated that limiting de-referencing to EU-domains and not conducting it on non-EU domains, including google.com, would not be sufficient; Article 29 Working Party (n 6) 9. Admittedly, it did not consider the possibility of EU-wide de-referencing in connection with geo-blocking. Similarly, the Italian data protection authority and the Supreme Court of Canada ordered a worldwide de-listing of search results; Bevilacqua (n 66) 656-7. Cf also Giancarlo Frosio, ‘Right to Be Forgotten: Much Ado About Nothing’ 15 Colorado Technology Law Journal 307, 332-333 (2017); Costanza Manavello and Laura Di Tecco, ‘The Global Implications of the CJEU’s Ruling in Google “Right to Be Forgotten” Case’ (IP Watchdog, 16 October 2019) <https://www.ipwatchdog.com/2019/10/16/global-implications-cjue-ruling-google-right-forgotten-case> accessed 3 December 2019.

68 Cf Frosio (n 67) 332.

69 Case C-507/17 Google v CNIL EU:C:2019:15, Opinion of AG Szpunar, para 36.

70 Padova (n 26) 26. Taylor even classifies global de-referencing as an example of unproductive jurisdictional overreach; Mistale Taylor, ‘Google Spain Revisited’ 3 European Data Protection Law Review 195, 206 (2017).

71 McCarthy (n 64) 10-11; Fomperosa Rivero (n 65) 43. In Jian Zhang v Baidu.Com Inc. [2014] 10 F. Supp. 3d 433. 72 This is reflected by the fact that while, in the EU, the right to data protection is enshrined in EU primary law (art 8 of the Charter), the US does not even have any horizontal data protection regulation on the federal level; cf. Nuala O’Connor, ‘Reforming the U.S. Approach to Data Protection and Privacy’ (2018) <https://www.cfr.org/report/reforming-us-approach-data-protection> accessed 2 December 2019.

73 This concern was explicitly mentioned by AG Szpunar, fearing that the cooperation mechanisms and instruments enshrined in the GDPR enable EU data protection authorities to adopt, where appropriate, EU-wide de-referencing.80 It can be derived that data protection authorities can also opt for de-referencing in only one or some Member States, e.g. in case the impact of the referencing of information on the rights and interests of the data subject is limited to certain Member States, or if in some Member States there is a substantially higher interest of the public in accessing such information.81 On the other

Nonetheless, as Advocate General Szpunar has put it, data protection is only one side of the coin.74 The other side of the coin represents the territoriality principle,75 and the right of other states to strike a different balance between the right to data protection and the freedom of information. It seems that the Court has tried to grant, in line with the principle of proportionality, the highest possible level of protection of the right to data protection while still respecting the named interests of other states, thereby trying to avoid any international tensions. In particular, a decision for EU-wide de-referencing aims to prevent a clash with the US system, where search engines enjoy free speech protection under the First Amendment to the US Constitution,76 while data protection does not enjoy such prominence.77 A request for global de-referencing could thus force tech companies to infringe upon protection of free speech in the US.78 On the other hand, the fear that a decision for global de-referencing could set a dangerous precedent and ‘return as a boomer-ang’ if authoritarian regimes also introduced such a right, blocking access to information in the EU, might also have contributed to the decision against global de-referencing.79

Even though the Court opted for EU-wide de-referencing as a ‘default choice’, it has left data protection authorities and courts some space for them to appropriately respond to the circumstances of a concrete case. It noted that the cooperation mechanisms and instruments enshrined in the GDPR reveal that the GDPR does have a substantial impact on data protection.82 The other side of the coin represents the territoriality principle,81 which aims to avoid any international tensions. In particular, a decision for EU-wide de-referencing aims to prevent a clash with the US system, where search engines enjoy free speech protection under the First Amendment to the US Constitution,76 while data protection does not enjoy such prominence.77 A request for global de-referencing could thus force tech companies to infringe upon protection of free speech in the US.78 On the other hand, the fear that a decision for global de-referencing could set a dangerous precedent and ‘return as a boomer-ang’ if authoritarian regimes also introduced such a right, blocking access to information in the EU, might also have contributed to the decision against global de-referencing.79

Even though the Court opted for EU-wide de-referencing as a ‘default choice’, it has left data protection authorities and courts some space for them to appropriately respond to the circumstances of a concrete case. It noted that the cooperation mechanisms and instruments enshrined in the GDPR enable EU data protection authorities to adopt, where appropriate, EU-wide de-referencing.80 It can be derived that data protection authorities can also opt for de-referencing in only one or some Member States, e.g. in case the impact of the referencing of information on the rights and interests of the data subject is limited to certain Member States, or if in some Member States there is a substantially higher interest of the public in accessing such information.81 On the other
hand, the Court also noted as an *obiter dictum* that while EU law does not require de-referencing on a global scale, it also does not prohibit such a practice. According to the Court, a national supervisory or judicial authority may, after balancing the rights and interests of the involved subjects in the light of national standards of protection of fundamental rights, order the search engine operator to carry out de-referencing on all versions of the search engine. In fact, in its press release following the Court’s decision, the CNIL explicitly highlighted this competence, yet acknowledged that it is competent to order worldwide de-referencing only ‘in some cases’. Admittedly, taking the spirit of the judgment into account, departing from the standard of EU-wide de-referencing is only possible in exceptional cases rather than in every case of de-referencing. Unfortunately, the Court has not provided any guidance hereto. Still, data protection authorities and courts shall be very vigilant when departing from the general rule of EU-wide de-referencing, carefully demonstrating why the circumstances of the case justify departing in one or another direction.

The procedural question whether a national data protection authority has to coordinate with other EU data protection authorities prior to deciding for global de-referencing was not explicitly answered by the Court. Zanfir-Fortuna argues that it does not have to. According to the view represented here, considering the statement of the Court that such a decision may be issued by ‘a national supervisory or judicial authority’, it cannot be inferred that the Court intended to exclude preceding coordination among the EU data protection authorities. Furthermore, if the EU data protection authorities have to coordinate when deciding for EU-wide de-referencing, they should *a fortiori* coordinate when deciding for global de-referencing, which also encompasses de-referencing in all EU Member States.

VI. Importance of the judgments for similar cases

As the main parts of the judgments in *GC and Others* and *Google v CNIL* focus on search engines, their transferability to other services is very limited. This especially holds true for the parts relating to the right to be forgotten. While the judgment is transferrable to other intermediaries such as social media and news portals, it is hardly imaginable that it would be directly transferrable to ‘normal’ webpages. For example, the balancing of the involved rights and interests and its outcome would be different if a journalistic or an artistic text were to be removed from the internet, rather than only a link to such a text.

In its argumentation pertaining to the processing of sensitive data (Art. 9 GDPR), the Court explicitly referred to search engine operators and their limited responsibilities, powers and capabilities. However, the assessment of the Court is generalizable. Therefore, in an attempt to be given the ‘privilege’ of only ex post application of prohibitions and restrictions enshrined in Art. 9 GDPR, companies in comparable situations, i.e. those not able to as ante and systematically assess and control what data will be processed by them (e.g. different web scrapers), might be able to refer to the judgment in *GC and Others* in similar legal proceedings.

On the other hand, the assessment pertaining to the territorial applicability of the GDPR, more specifically to Art. 3(1) GDPR, is of a more general nature. Numerous other companies located outside the EU might process the personal data of users in the EU themselves while having a branch or a subsidy in the EU responsible for promotional, advertising or similar activities. Nonetheless, the significance of the Court’s interpretation is limited due to the fact that even in absence of such an interpretation, the GDPR could in most cases also be applicable pursuant to Art. 3(2) GDPR.

VII. Conclusion

While the Court is known for its hard stance regarding the right to data protection, its decisions in *Google v CNIL* and *GC and Others* could be seen as lowering that protection. Namely, the Court did not opt for global de-referencing – the only mechanism capable of guaranteeing complete protection of the right to data protection – and considered the processing of sensitive data by a search engine operator lawful until obtaining a request for de-referencing, even without one of the exceptions enshrined in Art. 9(2) GDPR being fulfilled. However, the decisions rather have to be understood as a

82 In a similar case, *Glawschings-Pietzsch*, which was decided only a few days after the judgment in *Google v CNIL*, the Court was asked whether an order to a host provider to delete unlawful content pursuant to art. 15(1) of the eCommerce Directive may have a worldwide effect. The Court answered in the affirmative, yet emphasising that it is for the Member States to ensure that their measures producing effects worldwide are consistent with the rules applicable at the international level; Case C-18/18 *Glawschings-Pietzsch* EU:C:2019:821, paras 49-53. Even though at first sight this decision seems to be in direct contradiction to *Google v CNIL*, where the Court opted for merely EU-wide de-referencing, according to the view represented here, this is not entirely the case. Namely, in the light of the fact that the posting was found unlawful by Austrian courts, the Court merely pointed to the competence of the referring court to order worldwide deletion, as it similarly did with its ‘opening clause’ in *Google v CNIL*. On the contrary, the decision shall not be read as allowing, or even demanding, worldwide deletion in every case. 83 Case C-307/17 *Google v CNIL* EU:C:2019:772, para 72. According to certain authors, the Court allowed the external application of de-referencing under national laws of EU Member States rather than under EU law, cf Monika Zalnieriute, ‘To Forget, but not Forgive: Why the CJEU’s Latest Ruling on Google and the “Right to Be Forgotten” is not at all a Win for US Tech Giants’ (*EJIL: Talk!*, 29 November 2019) <https://www.ejiltalk.org/to-forget-but-not-forgive-why-the-cjeus-latest-ruling-on-google-and-the-right-to-be-forgotten-is-not-at-all-a-win-for-us-tech-giants/> accessed 2 December 2019; Olivier Proust and Alix Bertrand, ‘European Court Limits the Right to De-Referencing to the EU Territory’ (*fieldfisher*, 3 October 2019) <https://privacylawblog.fieldfisher.com/2019/european-court-limits-the-right-to-de-referencing-to-the-eu-territory/> accessed 2 December 2019. According to the view represented here, the Court rather allowed global de-referencing under the GDPR, but based on national standards of protection of fundamental rights. 84 *CNIL*, ‘“Right to be forgotten”: the CJEU ruled on the issue’ (*Commission Nationale de l’Informatique et des Libertés*, 24 September 2019) <https://www.cnil.fr/en/right-to-be-forgotten-cjeu-ruled-issue/> accessed 4 December 2019. 85 Some authors expressed concerns that in the future some data protection authorities would request de-referencing on a global scale, others EU-wide and others only nationally; cf, for example, Gstrein (n 70). However, a data protection authority cannot decide for one option to be used in all cases. Its decision for one of the options shall always respond to the circumstances of a specific case. Furthermore, the obligation of data protection authorities to use cooperation mechanisms and instruments provided for by the GDPR minimises the risk of arbitrary application of the law. 86 Zanfir-Fortuna (n 70). 87 Cf art 29 Working Party (n 6); Golland (n 18) 236. 88 Case-C-136/17 *GC and Others* EU:C:2019:773, para 47. 89 Golland (n 18) 236.
further adaptation of EU data protection law to the reality of the internet. As such, they have significant practical and political motivations. The practical motivation of the decision in GC and Others is that if the Court interpreted the GDPR rigidly, Google’s search engine and possibly numerous other search engines would be (i.e. continue to be) partially illegal – an outcome desirable neither for the Court nor for the numerous users of Google’s search engine in the EU. As to the decision in Google v CNIL, the Court was at least partially motivated by considerations regarding the political and legal impact global de-referencing could have on an international scale. The decision further demonstrates the incompatibility of the principle of territoriality with global data flows and underlines the need for a coherent theory of jurisdiction in the internet, including rules on the conflict of laws.

The decisions demonstrate yet again how difficult it is to draw lines in the internet and will have significant implications not only for internet users, but especially for tech companies in and outside the EU, as many aspects of the judgments directly affect their business models. Furthermore, as the Court is a pioneer when it comes to the right to be forgotten, the decision might also indirectly affect the legislation and court decisions in non-EU States.

By refraining from making absolute statements, the Court has deliberately left some space for data protection authorities to appropriately react to the specific circumstances of every case. In principle, this more nuanced approach is to be welcomed. However, while the obligation of data protection authorities to cooperate when issuing a decision lowers the risk of fragmented decision-making, such an approach might lead to further legal proceedings as to the scope of the right to be forgotten. Therefore, the Court might soon need to deal with the de-referencing of search results again.

90 Cf Finck (n 78).