HOW CAN WE FORGET ABOUT THIS? RIGHT TO BE FORGOTTEN IN THE LIGHT OF CJEU'S FACEBOOK AND GOOGLE CASES

Aleksander Wiatrowski

University of Lapland, Faculty of Law, Institute for Law and Informatics
Yliopistonkatu 8, 96300 Rovaniemi, FI
aleksander.wiatrowski@ulapland.fi, http://www.ulapland.fi/EN/Units/Institute-for-Law-and-Informatics

Keywords: ***right to be forgotten, privacy, data protection, facebook, google, CJEU***

Abstract: *Since in 2014 the famous Google Spain Case[1] promoted the term Right to be Forgotten (RTBF) discussions and controversies have never stopped. Recent 2019's rulings by the European Court of Justice (CJEU) in Facebook[2] and Google[3] cases not only did not dispel some of the doubts, especially those about territorial scope of the RTBF but raised more questions and uncertainties. The court found that Facebook is required to delete content globally, not just in Europe if a European court decides that the content is defamatory. This ruling is almost the exact opposite of a recent Google case. Google is required to delist links under RTBF in EU but does not need to delist that same material around the globe. How to reconcile these two decisions? Is one of them wrong or the reason is the difference in the companies, Facebook and Google? However, the surprises continue. Specifically, because the EU's E-Commerce Directive[4] prohibits Member States from imposing general monitoring obligations on social media sites and other online providers. Government-imposed monitoring raises an array of privacy-related concerns in addition to the obvious speech concerns. Something that one would think the EU would be particularly concerned about, given its strong focus on protecting individual privacy and data protection.*

1. Introduction

In 2014, the CJEU developed the jurisprudence establishing the European legal right to be forgotten[5] also referred to as the right to de-reference or delist. It allows individuals in the EU to request search engines to remove links containing personal information from web results appearing under searches for their names.[6] In that judgment, the Court also highlighted that the right is not absolute and is granted when one's personal data protection rights outweigh the public's interest in continued access to the information.[7]

Five years after the development of this legal framework in Google Spain Case, the territorial scope of this right continues to confuse the individuals seeking to enforce it and controllers of processed data receiving requests to de-reference. Notably, National Data Protection Authorities tasked with monitoring the application of the Directive within their territories and national courts have faced serious difficulties in interpretation.[8] The uncertainty of its scope prompted France's Conseil d'État[9] to seek clarifications from the CJEU.

---

1 Judgment of 13 May 2014, *Google Spain*, C-131/12, EU:C:2014:317.
2 Judgment of 3 October 2019, Glawischnig-Piesczek, C-18/18, EU:C:2019:821.
3 Judgment of 24 September 2019, *Google* v. CNIL, C-507/17, EU:C:2019:772.
4 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 («Directive on electronic commerce»), OJ L 178.
5 *Google Spain*, C-131/12.
6 *Google Spain*, C-131/12, para. 93.
7 Article 17 of the GDPR.
8 *Google* v. CNIL, C-507/17, para. 39.
9 Conseil d'État, (French: «Council of State»), highest court in France for issues and cases involving public administration, https://www.conseil-etat.fr/en/.

2. Google Case – Google v. CNIL, C-507/17 – Background

The case concerned a dispute between Google Inc. and CNIL, the French DPA, with regards to the scale on which de-referencing is to be given effect. In 2015, CNIL notified Google that it must apply the removal of links from all versions of its search engine worldwide. It held insufficient both measures implemented by Google to comply with the Directive: 1) delisting links from all EU and EFTA extensions, and 2) delisting links from all searches conducted in the French territory.

CNIL argued that internet users located in France are still able to access the other versions outside the EU (e.g. Google.com). Therefore, removing links about an individual residing in France only from the French version (google.fr) or even from versions in the other EU Member States is not enough to protect the individual's right, violating the Directive.

Google refused to comply and continued to limit its de-referencing of links only on search results conducted in the versions of its search engines with domain extensions within the EU and EFTA and used geoblocking, a measure which prevents the links from showing in searches made in France regardless of the version used. Google appealed to the Conseil d'État seeking to annul a 100,000 euro fine imposed by CNIL. The Conseil d'État, noting «several serious difficulties regarding the interpretation of the directive,»[10] subsequently referred questions to the Court of Justice for a preliminary ruling concerning the scope of application of Articles 12(b) and 14(a) of the Directive.

The search engine operated by Google is broken down into different domain names by geographical extensions (.fr, .de, .com, etc.). Where the search is conducted from «google.com», Google automatically redirects that search to the domain name corresponding to the State where the search is done. Google utilizes different factors such as the IP address to determine the location of a user performing a search on Google. The search engine will provide different results depending on the domain name extension and location (e.g. through IP address) of the user.[11]

The Court addressed whether EU data protection law on de-referencing should be interpreted to mean that a search engine operator is required to remove links: 1) on all versions of its search engine (worldwide), or 2) only on the versions corresponding to all Member States (within the EU), or 3) only on the version corresponding to the Member State of residence of the person requesting the de-referencing.[12]

2.1. Judgment of 24 September 2019, Google v. CNIL, C-507/17

Although the questions were referred from the point of view of Directive 95/46, the Court took General Data Protection Regulation 2016/679 into account, to ensure that its answers will be of use to the referring Court.[13]

The Court of Justice held that there is no obligation under EU law for Google to apply the European right to be forgotten globally.[14] The decision clarifies that, while EU residents have the legal right to be forgotten, the right only applies within the borders of the bloc's 28 Member States.

The Court referred to the objective of ensuring a high level of protection of personal data in the EU, pursued by both Directive 95/46 and Regulation 2016/679. It further admitted that a de-referencing carried out on all the versions of a search engine would meet that objective in full and argued that the EU legislature enjoys competence to lay down such an obligation.[15] The Court considered that the EU lawmakers had not done so,

[10] *Google* v. CNIL, C-507/17, para. 39.
[11] *Google* v. CNIL, C-507/17, para. 36.
[12] *Google* v. CNIL, C-507/17, para. 43.
[13] Although the Data Protection Directive was applicable on the date the request for a preliminary ruling was made, it was repealed with effect from 25 May 2018, from which date the GDPR is applicable. Therefore, the Court examined the questions in light of both the Directive and the GDPR to ensure that the decision will be of use to the refering court.
[14] *Google* v. CNIL, C-507/17, para. 64.
[15] *Google* v. CNIL, C-507/17, para. 58.

thus far. In consequence, for the time being, EU data protection law does not require search engine operators to carry out a de-referencing on all world-wide versions of a search engine. However, the Court also did not exclude a possibility for a supervisory or judicial authority of a Member State to weigh up, in the light of national standards of protection of fundamental rights, a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, where appropriate, to order such de-referencing.[16]

The Court began by observing that, in principle, de-referencing is to be carried out in respect of all Member States[17] and, if necessary, the search engine operator should be obliged to take sufficiently effective measures to ensure the effective protection of the data subject's fundamental rights. Actions of this kind should have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question while searching on the basis of that data subject's name.[18]

The Court left the question open whether automatic redirecting to a different national version of the search engine's website constitutes such a measure. It would seem that such blocking or redirection would then fall under the exception to customers' right of access to online interfaces, set out in Article 3(3) of Regulation 2018/302 on geo-blocking[19].

The Court accepted that the interest of the public in accessing information might, even within the Union, vary from one Member State to another, meaning that results of the balancing exercise are not necessarily the same for all the Member States. The Court thus emphasized the role of cooperation between supervisory authorities in the Member States as an adequate framework for reconciling the conflicting rights and freedoms. It is through this framework, therefore, that a de-referencing decision, covering all searches conducted from the territory of the Union based on a data subject's name, should be adopted.[20]

3. Facebook Case – Glawischnig-Piesczek, C-18/18 – Background

The whole case centres around Eva Glawischnig-Piesczek, a chairperson for the Greens party in Austria. A private citizen in Austria shared an article on Facebook about Glawischnig-Piesczek and called her a «lousy traitor of the people» and a member of a «fascist party,» among other names. The article appeared on the Austrian news website oe24.at and was titled, «Greens: Minimum income for refugees should stay.»[21]

The decision stems from a reference for a preliminary ruling made by the «Oberster Gerichtshof» (Austrian Supreme Court), in a case considering an appeal by both Eva Glawischnig-Piesczek – a member of the «Nationalrat» (House of Representatives of the Parliament, Austria), chair of the parliamentary party «die Grünen» (The Greens) and federal spokesperson for that party – and Facebook Ireland, challenging a decision by the lower court, «Oberlandesgericht Wien» (Higher Regional Court, Vienna). In that case, Glawischnig-Piesczek sued Facebook before the Austrian courts, requesting that Facebook Ireland be ordered to remove a comment deemed harmful to her reputation, published by a user on that social network, and any identical or equivalent content.

The Austrian Supreme Court asked the CJEU for clarification concerning the interpretation of Article 15(1) of the so-called E-Commerce Directive, which provides as follows: Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the infor-

16 *Google* v. CNIL, C-507/17, para. 72.
17 *Google* v. CNIL, C-507/17, para. 66.
18 *Google* v. CNIL, C-507/17, para. 70.
19 Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, OJ L 60I.
20 *Google* v. CNIL, C-507/17, para. 69.
21 Glawischnig-Piesczek, C-18/18, para. 12.

mation which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

In particular, the Austrian Supreme Court asked whether Article 15(1) of the E-Commerce Directive should be interpreted as precluding a court of a Member State from being able to: 1) order a hosting provider to remove or disable access to information, which it has stored and the content of which is identical to that of information which has previously been declared illegal, irrespective of who requested the storage of that information; and 2) order a hosting provider to remove or disable access to information, which it has stored and the content of which is equivalent to that of information which has previously been declared illegal; and 3) extend the effects of such an injunction worldwide.[22]

3.1. Judgment of 3 October 2019, Glawischnig-Piesczek, C-18/18

The Court started its analysis by making clear that the immunity from suit granted by Article 14 of the E-Commerce Directive is not a general immunity from every legal obligation. Specifically, the national authorities remain competent to require a host to terminate access to or remove illegal information. The Court also noted that Article 18 of the E-Commerce Directive requires Member States to have in place appropriate court actions to deal with illegal content. The Court held that no limitation on the scope of such national measures could be inferred from the text of the E-Commerce Directive.[23]

According to the Court, Member States enjoy broad discretion concerning to actions and procedures for taking necessary measures.[24] Such a margin of discretion is due to, among others, the rapidity and geographical extent of the damage arising in connection with information society services. Both of these factors were also clearly at play in the present case.[25]

The Court decided to distinguish between injunctions concerning information whose content is identical to the one which was previously deemed illegal and injunctions concerning information with equivalent content – whose message remains essentially unchanged and therefore diverges very little from the content which gave rise to the finding of illegality.[26] When it comes to information with equivalent content the Court sought a balanced solution. It considered that injunctions should generally be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal.[27]

The CJEU highlighted the fact that while Article 15 of the E-Commerce Directive prohibited general monitoring as recital 47 in the preamble of the Directive makes clear, monitoring «in a specific case» does not fall within that prohibition. It then held that such a specific case might, in particular, be found, as in the main proceedings, in a specific piece of information stored by the hosting provider concerned at the request of a certain user of its social network.[28]

The Court determined an equivalent meaning to be about the message the information posted conveys and which was essentially unchanged. Given the focus on meaning not form, the Court held that an injunction could extend to non-identical posts as otherwise the effects of an injunction could easily be circumvented. The Court then considered the balance between the competing interests and commented that the equivalent information identified by court order should contain specific elements to identify the offending content and in

22 Court of Justice of the European Union, PRESS RELEASE No 128/19, Luxembourg, 3 October 2019.
23 Glawischnig-Piesczek, C-18/18, para. 30.
24 Glawischnig-Piesczek, C-18/18, para. 29.
25 Glawischnig-Piesczek, C-18/18, para. 36.
26 Glawischnig-Piesczek, C-18/18, para. 39.
27 Glawischnig-Piesczek, C-18/18, para. 41.
28 Glawischnig-Piesczek, C-18/18, para. 35.

particular must not require the host to carry out its independent assessment. In terms of assessing the burden on the host, the court noted that the host would have recourse to automated search tools and technologies.[29]

As regards territorial scope, the Court once again confirmed the broad reading of Article 18(1), E-Commerce Directive, which did not make provision for any limitation, including a territorial limitation, on the scope of the measures which Member States are entitled to adopt.[30] The Court also noted that Article 18 of the E-Commerce Directive makes no provision for territorial limitations on what measures Member States may make available. In principle, world-wide effects would be permissible[31], but this is subject to the proviso that EU rules must be consistent with the international law framework – Member State courts may order platforms to take down illegal content and ensure that identical and equivalent content is also taken down. The effect of such orders may extend globally, subject to compliance with relevant international law, which is for the Member State courts to assess.

4. Comparing Case C-507/17 with Case C-18/18

Both Google v. CNIL and the Facebook Ireland cases tackle the same legal question, namely the territorial effect of removal of information. However, the legal frameworks of these cases were presented differently.

In both cases, the CJEU begins its reasoning by reading into the E-Commerce Directive and the GDPR, respectively, the wish of the EU legislature to strike a balance between the interests at stake.[32] In the Facebook case, the interest of the person seeking to have defamatory content taken down is balanced against the difficulty of the hosting provider to comply with a measure in respect of the E-Commerce Directive. In the Google case, the interest of the person seeking to take down content infringing his data protection rights is balanced against the right to freedom of information which evidently is adversely affected by a de-referencing order in respect of the GDPR.

In the Google case the CJEU reasons that while EU legislature has struck a balance between the right to privacy and the right to freedom of information[33] as regards the application of the right to be forgotten within the EU, it has not struck such a balance as regards application outside the EU territory.[34] The reason is that the rights arise from the EU Charter of Fundamental Rights.

The CJEU holds that GDPR does not indicate any of its provision should apply outside of the EU territory. Therefore, it is only required to be given effect within the territory of the EU.[35] However, the CJEU argues that neither does the GDPR expressly prohibit its application worldwide.[36] While the fact that EU law does not require extraterritoriality, the GDPR's silence on the point gives space to a national court to make an order with extra-territorial effect. In Google v. CNIL, while the Court recognised the possibility for national courts to make orders for de-referencing with extra-territorial effect, it expressly noted that in doing so they must weigh up the competing interests of the data subjects and the right of others to freedom of information.[37] It is noticeable that in Glawischnig-Piesczek the balancing is different. The Court notes the subject's interest in the information and also the need not to impose an excessive burden on the hosting provider.[38] The existence of other rights: the right of the host to carry on a business and the rights of those posting the material and those wishing to receive it – both aspects of freedom of expression – are not expressly mentioned.

---

29 Glawischnig-Piesczek, C-18/18, para. 46.
30 Glawischnig-Piesczek, C-18/18, para. 49.
31 Glawischnig-Piesczek, C-18/18, para. 50.
32 *Google* v. CNIL, C-507/17, para. 60, Glawischnig-Piesczek, C-18/18, para. 43.
33 See Article 17(3)(a) of the GDPR.
34 *Google* v. CNIL, C-507/17, para. 61.
35 *Google* v. CNIL, C-507/17, para. 62 and 63.
36 *Google* v. CNIL, C-507/17, para. 72.
37 *Google* v. CNIL, C-507/17, para. 72.
38 Glawischnig-Piesczek, C-18/18, para. 45 and 46.

To some extent, the issue of rights will be covered through the national courts, which will be the bodies to carry out that balancing within their national frameworks and the limits of EU law. By contrast to Google v CNIL, however, there is no instruction from the Court that these are matters to be considered, nor any express recognition that the balance between the right to private life, including the protection of reputation and freedom of expression differs between territories. What might be seen as the legitimate protection of private life in one place is an infringement of speech in another.

In the Facebook case, the CJEU simply states the balance of the individual's and the host provider's interests must mean that the hosting provider cannot be burdened with an excessive obligation, that is, a hosting provider cannot be obliged to monitor for an illegal activity generally.[39] In fact, the Member States are expressly prohibited from imposing such a general obligation by Article 15 of the E-Commerce Directive; therefore, a balance struck in this sense is purely made in terms of EU legislation and, by implication, cannot be applied to measure which affect worldwide.

The CJEU posits that nowhere does the E-Commerce Directive make any territorial limitation to the application of the measures permitted under Article 18, therefore, those measures may be given worldwide effect.[40] Nevertheless, in the case that a Member State applies a measure with the worldwide effect, it must do so in a manner consistent with the framework of the relevant international law.[41]

The effect of the two cases is the convergence of the territorial scope of the GDPR and the E-Commerce Directive. However, a balance must then be struck between the interests at stake. In the case of the GDPR, it is about national standards of fundamental rights' protection. In the case of the E-Commerce Directive, it is about international law.

5. Conclusion

Google v CNIL is a long-awaited clarification of, at the very least, the geographical boundaries of the right to be forgotten. As the Court held, there is little room for interpretation under the current legal framework of data protection to establish a global application of such a right. It highlighted the difficulties of global de-referencing noting that public interest in access to information substantially varies among third States. Therefore, the balancing of fundamental rights would also differ. The Court went on to say that the EU framework does not provide for cooperation instruments and measures outside its territory and chose the EU-wide approach. The decision is critical because, at first glance, it appears to have closed the door for EU residents to demand a worldwide removal of their information, in certain circumstances, from search engine results under the GDPR. The Court explicitly set limits on the territorial scope of an individual's right to de-reference. In simple terms, this means that Google is only required to remove links to personal data from internet searches conducted within the EU.

On the other hand, just because the law stands as it currently does, it does not mean that it is adequate. By explicitly limiting the territorial scope of the right to be forgotten, the Court may seem to have inadvertently limited the impact and protective effect of this right. Given the importance of a global application of the right, allowing internet users conducting searches outside the EU to still be able to access the links de-referenced in the EU after this judgment will potentially undermine the right to be forgotten and weaken the protection sought to be achieved by the right or, at the minimum, the Union's objective of guaranteeing a high level of protection of personal data cannot be fully met. The CJEU's decision provided clarity on the scope of the right under EU law, it also left areas of uncertainty. For example, since the Court left the option open for DPAs to determine the conditions which will justify a delisting on all versions of a search engine based on national

[39] Glawischnig-Piesczek, C-18/18, para. 43.
[40] Glawischnig-Piesczek, C-18/18, para. 49 and 50.
[41] Glawischnig-Piesczek, C-18/18, para. 51.

standards of the protection of fundamental rights, it is expected that the CJEU will continue to see more questions about the global reach of the EU's data protection.

In light of all of this, it is a missed chance to develop individual rights in the digital age further, promoting human dignity in the digital age. It is justified to state that the Court has failed to recognize its mission and mandate.

There are also some other immediate issues to mention. In both cases, the Court emphasises the need to act «within the framework of the relevant international law». The problem is the lack of consistent and sufficient international law in these matters. In general, the CJEU's approach is very much aligned with the US, Supreme Court of the United States in particular, judicial approach in similar extraterritoriality issues, such as sanctions law or export controls.[42] However, as prof. Svatesson points out,[43] the Austrian court may now force Facebook to prevent future publications, that may originate in the US and be lawful there, with worldwide effect. Now re-read that sentence replacing «Austrian» with «Chinese», and «US» with «EU». I can only imagine that the Court's ruling is likely to infuriate US lawyers worried about its impact on freedom of speech.

The Court recognizes the concern about general monitoring but says that is addressed if there is sufficient clarity as to what kinds of equivalent content would qualify. According to the Court, if there is sufficient clarity, then companies like Facebook would be freed from having to make the kind of independent assessment that would raise concern. They could simply carry out the takedown requirements with automated search tools and technologies. However, it is not entirely clear how companies are supposed to determine what is identical unless the criteria for this is limited to shares of the precise post with the precise picture and precise words.[44] The court is presuming a level of technological sophistication and degree of specificity that simply do not, and likely never will exist. Even applying this to identical posts is challenging.

The judgment of the Court in the Facebook case has some implications. It strengthens the protection of parties affected by illegal content but seeks to achieve this without undermining the validity of E-Commerce Directive Article 15. As such, it does not provide a straightforward solution to each and every future case and sets quite demanding requirements for both national courts and host providers. The judgment is relevant beyond the social media context but can also be applied to other platforms like online marketplaces. Operators of such platforms could be required to take steps to monitor their content e.g. as regards the recurring presence of misleading information.

Of course, one cannot help noticing the similarity between the question of territorial scope addressed Google and Facebook cases.

In Glawischnig-Piesczek, the Court did not provide for an equally balanced framework but limited itself to stating that injunctions with worldwide effects are not precluded by E-Commerce Directive. This remains in line with the opinion of Advocate General Szpunar[45] – the same AG whose advice was followed in the Google case. Both findings are, not necessarily inconsistent. The opinion in Glawischnig-Piesczek explicitly refers to the Google case. According to the AG, like with the right to be forgotten, «the legitimate public interest in having access to information will necessarily vary, depending on its geographic location, from one-third State to another».[46] Consequently, the limitation of extraterritorial effects of injunctions concerning

[42] Van Calster G., Steady now. Eva Glawischnig-Piesczek v Facebook. The CJEU on jurisdiction and removal of hate speech, Conflict of Laws /Private international law, EU law – General, October 10, 2019, https://gavclaw.com/tag/c-13617/.

[43] Svatesson D., Bad news for the Internet as Europe's top court opens the door for global content blocking orders, October 3, 2019, https://www.linkedin.com/pulse/bad-news-internet-europes-top-court-opens-door-global-svantesson/.

[44] Daskal J., A European Court Decision May Usher In Global Censorship, 3 October, 2019, https://slate.com/technology/2019/10/european-court-justice-glawischnig-piesczek-facebook-censorship.html.

[45] Opinion of Advocate General Szpunar delivered on 4 June 2019, Glawischnig-Piesczek, C-18/18, EU:C:2019:458.

[46] Opinion of Advocate General Szpunar, para. 99.

harm to private life and personality rights, for example by way of geo-blocking, may remain «in the interest of international comity».[47]

It is important for the CJEU to provide clarity on the territorial extent of removal requests and to ensure the effective protection of personal data at the same time. It would not be preferable for the Court to create a general rule because such a rule does not fit in the system of the balancing test. A general rule to remove information on a worldwide level would, in some cases, disproportionally harm the freedom of access to information of people outside the EU. On the other hand, a general rule that information only has to be removed within the EU, hence geographical restricted, will not protect the privacy of data subjects in certain cases. I believe that a national judge should have the freedom to decide on a case level whether specific information can be removed globally or locally.

To partially answer my initial question about the general differences in the two Court's judgment I would like to say that, yes to a certain point the characteristics of both companies, Facebook and Google, matter. As a result, the Court used different balancing. The question is, can national courts use both balancing test in one case in the future? One thing I find quite certain. In both cases, the Court rules that EU law – privacy law in the case of Google v. CNIL, platform liability law in the case of Glawischnig-Piesczek – does not prevent national courts in EU member states from ordering the delisting or the takedown of content globally. However, while the Google case left open the legal basis for such rulings, inviting further litigation on that matter under national law, the Facebook case is quite clear about deferring.

47 Opinion of Advocate General Szpunar, para. 100.