Google v. CNIL and *Glawischnig-Piesczek v. Facebook*: content and data in the algorithmic society

Giovanni De Gregorio

Court of Justice of the European Union, 24 September 2019, C-507/17, *Google v Commission nationale de l'informatique et des libertés (CNIL)*

Court of Justice of the European Union, 3 October 2019, C-18/18, *Eva Glawischnig-Piesczek v. Facebook Ireland*

Almost at the end of 2019, two decisions of the Court of Justice of the European Union ("CJEU") have shed the lights on some problematic points in the field of data and content. In *Google v. CNIL*, the Luxembourg Court addressed the boundaries of the territorial scope of application of the right to be forgotten online. In *Glawischnig-Piesczek v. Facebook*, the CJEU addressed whether removal obligations can be extended to identical and equivalent content as well as their territorial scope of application. In the first case, the CJEU recognised that search engines are not required to delist links and information globally, but Member States can still decide to extend their orders to all the domain names of the search engine in question. The second case acknowledges that removal obligations of illicit content also extend to identical and equivalent content. Concerning the territorial scope of application, this case recognises that EU law does not preclude Member States to require hosting providers to remove content on a global scale. The two decisions share points of convergence and divergence. On the one hand, both cases deal with the activities of two of the most relevant online platforms like Facebook and Google and the territorial scope of judicial and administrative orders of removal. On the other hand, the decision underlined how the legal regime of data and content are based on different pillars and the differences in these two decisions show this constitutional distinction which, however, is going to converge in the algorithmic society.

Summary

Keywords

freedom of expression - data protection - Court of Justice - right to be forgotten - content moderation

1. Introduction

Almost at the end of 2019, two decisions of the Court of Justice of the European Union ("CJEU") have shed the lights on some problematic points in the field of data and content. In *Google v. CNIL* ("*Google* case"),[1] the Luxembourg Court addressed the boundaries of the territorial scope of application of the right to be forgotten online. In *Glawischnig-Piesczek v. Facebook* ("*Facebook* case"),[2] the CJEU addressed whether removal obligations can be extended to identical and equivalent content as well as their territorial scope of application.

The relevance of these decisions can be understood if they are framed within the Union where there is an increasing (regulatory) attention over content and data. In the last years, the Digital Single Market strategy has led to the introduction of new legal instruments to address the challenges for freedom of expression and personal data in the information society. In the field of content, the Union has introduced new rules addressing platforms' activities. This approach is still primary when looking at the Directive on Copyright in the Digital Single Market,[3] and the amendments in the framework of the Audiovisual Media Service Directive.[4] Likewise, in the field of data, the General Data Protection Regulation ("GDPR"),[5] as well as the Proposal for a Regulation on Privacy and Electronic Communications,[6] reviewed the EU privacy and data protection legal framework increasing the degree of uniformity between Member States' legislation.

However, addressing the issues in the field of content and data is not a neutral activity from a constitutional law perspective. It concerns the protection of two fundamental rights which are increasingly challenged when focusing on online platforms' activities of content moderation and processing of personal data through automated decision-making systems. Content moderation and data processing are two fundamental pieces of the jigsaw showing how online platforms do not exercise a passive role in the algorithmic society. Decisions regarding the expressions of billions of users on a transnational scale and definition of new automated decision-making techniques based on profiling contribute to defining standards of protection of fundamental rights extending well beyond national borders, thus, affecting the principle of the rule of law.

[1] CJEU, C-507/17, *Google CNIL* (2019).

[2] CJEU, C-18/18, *Eva Glawischnig-Piesczek* (2019).

[3] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[4] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[6] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

Indeed, the private governance of content and data on a global scale does not only concern the protection of fundamental rights such as freedom of expression, privacy or human dignity. It also influences concepts such as territory and sovereignty due to the involvement of different legal systems whose extension question the traditional limits characterising public powers exercised on a given territory.

2. Data: The Decision in *Google v. CNIL*

Within this framework, the CJEU ruled on a preliminary reference concerning the territorial scope of the right to be forgotten online in September 2019. The case initially arose from a formal notice which the President of the CNIL submitted to Google requiring the search engine to delist information of data subjects from all its domain name extensions. Google refused to comply with such a request arguing that the removal of links in the case in question could just concern the results from the domain names of its search engine in the Member States. Google also proposed the application of geo-blocking measures according to which users would have been prevented from accessing the results from an IP address deemed to be located in the State of residence of a data subject, no matter which version of the search engine they used.
Nevertheless, the CNIL decided that Google failed to comply with the formal notice and, therefore, sanctioned Google with a penalty of 100000 euros. In the phase of appeal before the *Conseil d'État*, the Court recognised the possibility for users to access Google's search engine domain names from French territory. Google complained that the CNIL's decision was based on the incorrect interpretation of the *Google Spain* decision.[7] According to Google, the aforementioned decision would not impose search engines to removes links without geographical limitation. Furthermore, such an approach would affect the principles of courtesy and non-interference recognised by public international law as well as undermining the protection of freedoms of expression around the world.
The point raised by Google about the vague boundaries of the *Google Spain* case led the *Conseil d'État* to submit a preliminary reference to the CJEU raising question about the scope of de-referencing orders according to the legal framework of Directive 95/46/EC ("Data Protection Directive"),[8] as also interpreted by the *Google Spain* decision. In particular, the French Court asked whether the delisting performed by a search engine should be global or limited to the domain name of the State in which the request is deemed to have been made or to the national extensions of all Member States, including the possibility to apply geo-blocking techniques in this last case.
As initial steps, the CJEU firstly clarified that, although the Data Protection Directive was in force on the date the request for the preliminary ruling, this legal instrument was repealed by the GDPR. Therefore, the Luxembourg Court took into consideration

[7] CJEU, C-131/12, *Google Spain* (2014).

[8] 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 dataData Protection

both measures to allow national courts to rely on an applicable interpretation. Secondly, the Luxembourg judges recalled the interpretation of the *Google Spain* decision concerning the role of fundamental rights of privacy and data protection in defining the scope of the right to the delist based on Art. 12(b), Art. 14(1)(a) of the Data Protection Directive,[9] and the notion of establishment based on the assessment of the context of activities involving the processing of personal data regardless of whether that processing takes place in the Union or not.[10]

Based on these assumptions, the CJEU observed that the scope of the Data Protection Directive and the GDPR is to guarantee a high level of protection of personal data within the Union and, therefore, a de-referencing covering all the domains of a search engine (i.e. global delisting) would meet this objective. This is because of the role of search engines in disseminating information is relevant on a global scale since users can access links to information «regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself».[11]

Nevertheless, the CJEU underlined the limits of this global approach. Firstly, States around the world do not recognise the right to delist or provide different rules concerning the right to be forgotten online.[12] Even more importantly, since the right to privacy and data protection are not absolute rights, they need to be balanced with other fundamental rights,[13] among which the right to freedom of expression.[14] The protection of these fundamental rights (and, therefore, their balance) is not homogenous around the world. Indeed, GDPR does not aim to strike a fair balance between fundamental rights outside the territory of the Union.[15]

Before this crossroads, the Luxembourg judges followed the opinion of the AG Spuznar,[16] thus, observing that neither the Data Protection Directive nor the GDPR recognises the right of data subjects to require a search engine like Google to delist content worldwide.[17] Therefore, although Google falls under the scope of EU data protection law, it is not required to delist information outside the territory of Member States. Nonetheless, Member States still maintains the possibility to issue global delisting order according to their legal framework. The Luxembourg judges specified that, if, on the one hand, EU does not require search engines to remove links and information globally, on the other hand, it does not ban this practice. It is for Member States to decide whether extending the territorial scope of judicial and administrative order according to their constitutional framework of protection of privacy and personal data

[9] C-131/12, cit., § 88, § 99.

[10] *Ivi,* §§ 56-60.

[11] C-507/17*,* cit., § 57.

[12] *Ivi,* § 58.

[13] *Ivi,* § 59.

[14] See, in particular, CJEU, C-92/09 and C-93/09, *Volker* (2010), § 48; Opinion 1/15 *(EU-Canada PNR Agreement)* (2017), § 136.

[15] GDPR, Art. 17(3)(a).

[16] Opinion of Advocate General in C-507/17, 10 January 2019, § 63.

[17] C-507/17, cit., § 64.

balanced with the right to freedom of expression.[18]

The CJEU also explained that the impossibility to require search engines to delist information on a global scale is the result of the lack of cooperation instruments and mechanisms in the field of data protection. The GDPR only provides the supervisory authorities of the Member States with internal instruments of cooperation to come to a joint decision based on weighing a data subject's right to privacy and the protection of personal data against the interest of the public in various Member States in having access to information.[19] Therefore, such instruments of cooperation cannot be applied outside the territory of the Union.

Regarding the second question concerning the territorial scope of delisting within the territory of the Union, the CJEU observed that the adoption of the GDPR aims to ensure a consistent and high level of protection of personal data in all the territory of the Union and, therefore, delisting should be carried out in respect of the domain names of all Member States.[20] Nonetheless, the Court acknowledged that, even within the Union, the interest of accessing information could change between Member States as also shown the degree of freedom Member States enjoy in defining the boundaries of processing in the field of freedom of expression and information pursuant to Art. 85 of the GDPR.[21] In other words, the CJEU underlined not only that freedom of expression does not enjoy the same degree of protection at the international level but also, in Europe, it can vary from one Member State to another. Therefore, it is not possible to provide a general obligation to delist links and information applying to all Member States.

To answer this issue, the Court left this decision to national supervisory authorities which through the system of cooperation established by the GDRP should, *inter alia*, reach «a consensus a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all its establishments in the Union».[22] Likewise, even concerning geo-blocking techniques, the CJEU did not interfere with Member States' assessment about these measures just recalling by analogy that "these measures must themselves meet all the legal requirements and 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 using a search conducted on the basis of that data subject's name".[23] By distances itself from the AG Spzunar's view on this point,[24] the Court decided not to recognise a general removal obligation at the EU level but relied on the mechanism of cooperation of national authorities as well as to the discretion of Member States concerning preventing measures.

---

[18] See CJEU, C-617/10, *Åkerberg Fransson* (2013), § 29; C-399/11, *Melloni* (2013), § 60.

[19] GDPR, Art. 56, §§ 60-66.

[20] C-507/17, cit., § 66.

[21] *Ivi,* § 67.

[22] *Ivi,* § 68.

[23] *Ivi,* § 70. See, *inter alia,* CJEU, C-484/14, *McFadden* (2016), § 96.

[24] Opinion of Advocate General in C-507/17, cit., § 78.

3. Content: The Decision in *Glawischnig-Piesczek v. Facebook*

Just two weeks later, the CJEU dealt with a preliminary reference concerning an online defamation case involving social media. The case concerned the former Austrian deputy of the *Nationalrat*, as well as president of the parliamentary group *die Grünen* and federal spokesman of the relative political party. She complained of an injury of her honour following the publication of a defamatory content accessible to every Facebook user. Since Facebook did not remove the content in question, the former deputy asked Austrian judges to order Facebook the removal not only of the defamatory content in question but also of the identical claims and equivalent content.

In 2016, the *Handelsgericht Wien* issued an interim order upholding the applicant's requests, thus, ordering Facebook to remove the message in question and the equivalent content. However, the *Oberlandesgericht Wien* restricted this possibility only to identical statements considering that Facebook would have been required to also remove equivalent statements only in case of awareness coming from the notice of the applicant, by third parties or otherwise. Before these opposite views, the *Oberster Gerichtshof* decided to refer some questions to the CJEU concerning the interpretation of e-Commerce Directive, in particular about Facebook responsibility to remove identical and equivalent expressions to hosted content based on the order of a national judge as well as concerning the territorial scope of this order.

Before these questions, the CJEU firstly underlined that Facebook falls under the scope of hosting providers and, as such, is subject to the rules of the Directive 2000/31/EC ("e-Commerce Directive").[25] Secondly, the Court underlined how, regardless of the liability exception provided for by Art. 14 and the prohibition for Member States to introduce monitoring obligations pursuant to Art. 15, hosting providers may be subject to orders from judges or administrative authorities to cease an infringement or prevent it through the removal or blocking of content. According to the Luxembourg judges, Member States cannot introduce measures leading to general monitoring obligations, but this ban does not apply «in a specific case».[26]

Based on these opening considerations, the CJEU focused on the first question, namely whether a hosting provider may be subject to an obligation to remove content identical and equivalent to that covered by the case in question. The Luxembourg judges underlined the role of social media in promoting the reproduction and dissemination of information online. This activity can also extend to content whose illegality has been determined by the judicial authority like in the case in question. Therefore, national judge's orders of removal or blocking of identical content do not conflict with

[25] 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.

[26] The Court had already specified these conclusions in other cases. See, in particular, CJEU, C-70/10, *Scarlet* (2011); C-360/10, *Netlog* (2012); C-314/12, *UPC Telekabel Wien* (2014), § 62. The CJEU adds that «[s]uch a specific case may, in particular, be found, as in the main proceedings, in a particular piece of information stored by the host provider concerned at the request of a certain user of its social network, the content of which was examined and assessed by a court having jurisdiction in the Member State, which, following its assessment, declared it to be illegal», § 35.

the monitoring ban established by the e-Commerce directive.[27] As the AG Spuznar underlines, an order to remove all identical information does not require "active non-automatic filtering".[28]

Having addressed the first point regarding identical content without particular critical issues, the CJEU addressed the question concerning the removal of "equivalent" content. According to the Court, in order to effectively cease an illegal act and prevent its repetition, the order of the national judge has to be able to also extend to "equivalent" content defined as «information conveying a message the content of which remains essentially unchanged and therefore diverges very little from the content which gave rise to the finding of illegality».[29] Otherwise, users would only access a partial remedy that could lead to resorting to an indefinite number of appeals to limit the dissemination of equivalent content.[30]

However, such an extension is not unlimited. Indeed, the CJEU reiterated that the ban on imposing a general surveillance obligation pursuant to Art. 15 is still the relevant threshold for Member States' judicial and administrative orders. If, on the one hand, the possibility of extending the orders of the national authorities to equivalent content aims to protect the victim's honour and reputation, on the other hand, such orders cannot entail an obligation for the hosting provider to generally monitor information to remove equivalent content. In other words, the Court does nothing but identify a balance between, on the one hand, the freedom of economic initiative of the platform, and, on the other, the honour and reputation of the victim. The result of such a balance, therefore, leads to reiterate that the national orders of the judicial and administrative authorities have to concern specific cases without being able to extend to the generality of the content hosted by the provider in question.

In order to balance these conflicting interests, the CJEU provided other conditions applying to equivalent content. In particular, expressions have to contain specific elements duly identified by the injunction like «the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal».[31] Under these conditions, the protection granted to the victim would not constitute an excessive obligation on the hosting provider since its discretion is limited to certain information without leading to general monitoring obligation that could derive from an autonomous assessment of the equivalent nature of the content.

Concerning the territorial extension of the national injunction, the Luxembourg judges observed that Art. 18 of the e-Commerce Directive does not provide for any limitation to the territorial scope of the measures that Member States can adopt and, consequently, EU law does not prevent a national order to extend the scope application of their measures globally. As a general limit, the CJEU specified that Member States should take into consideration their international obligations given the global dimen-

[27] C-18/18, cit., § 37.

[28] Opinion of Advocate General in C-18/18, cit., § 61.

[29] C-18/18, cit., § 39.

[30] *Ivi,* § 41.

[31] *Ivi,* § 45.

sion of the circulation of content, without either however specifying which rules of international law would apply in this case.

4. Content and Data on a Global Scale

These two decisions deserve to be analysed together for several reasons whose relevance emerge in the following considerations. Apart from similarities and differences, both decisions contribute to shaping the legal regimes of data and content at EU level providing new pieces of the jigsaw. Nevertheless, at the same time, the two decisions also introduce new questions and concerns, thus, extending the size of the puzzle of the legal regime of content and data in the Union.

By firstly focusing on the Facebook decision, it is possible to observe how this case is divided into two main sections. The first part deals with the boundaries of the monitoring ban pursuant to Art. 15 of the e-Commerce Directive relating to the power of national judges to order hosting providers to remove identical and equivalent content. The second point goes well beyond the first question and focuses on the limits of the territorial scope of the removal order. In other words, the Luxembourg judges were asked to clarify whether EU law does not prevent national courts and administrative authorities from ordering a hosting provider, such as Facebook, that had not promptly delete illegal information, to remove, not only the above illegal information but also identical and (or alternatively) equivalent information on a global scale.

From the first point of view, it is worth observing that the scope of the case would not generally cover all content hosted on Facebook, but just expressions defined illegal by national authorities. The e-Commerce Directive does not subject the obligation of platforms to remove content to the prior scrutiny of public authority concerning its unlawfulness. Unlike, for example, the Italian Legislative Decree 70/2003, whose Art. 15 implementing Art. 14 of the e-Commerce Directive, subjects the removal obligation to the preliminary assessment of the public authority. In the lack of such public filter, it is not clear whether hosting providers can be required to remove or block identical and equivalent content based merely on users' request or users need to rely on the order of a public body. Furthermore, since the lack of harmonisation in the field of defamation, this approach could lead users to bring their cases where national authorities tend to restrict more freedom of expression and issue global take-down orders (i.e. forum shopping).

This vagueness also extends to the characteristics of "identical" and "equivalent" content which the CJEU has not clearly defined, thus, leaving broad margins of discretion to national authorities in interpreting these notions. As Savin underlines, "the AG's opinion allows the monitoring to take place on all the information of all the users on the platforms for "identical" information but only on the disseminator's account for "equivalent" information. This is both justified and reasonable. No such distinction exists in the Court's judgment, which allows monitoring for both identical and equivalent".[32] Likewise, there is no reference to what kind of preventive measures a national

[32] A. Savin, *The CJEU Facebook Judgment on Filtering with Global Effect: Clarifying Some Misunderstandings*, in

order can require to social media. Husovec has stressed that "the key thing about this case is what preventive measures can be imposed on Facebook".[33]

However, the discretion of public actors is not the only concern at stake. It is worth observing that, in the digital environment, online platforms can play a crucial role in the interpretation of legal requirements in their activities of content moderation.[34] When deciding on the removal or block of "identical" or "equivalent" content, Facebook will, therefore, decide in which cluster a certain expression would fall. This activity is an example of how online platforms contributes to defining the standard of protection of rights and freedoms online whose borders are strictly influenced by decisions of private actors. The Facebook decision does not take into consideration the consequences that certain choices can entail for the protection of fundamental rights in the digital context. It is no secret that content moderation is carried out not only by human moderators around the planet in regions that are also very distant from the context of moderate content. This activity is also performed by artificial intelligence systems that signal, and sometimes decide, the fate of billions of content online. In the latter case, the use of automated systems for content moderation could also increase the risk of arbitrary removal due to the bias as well as errors that could occur in the definition of identity or equivalence of the content in question. Therefore, it will be the set of decisions made by artificial intelligence systems and moderators to catalogue content as "identical" or "equivalent" and, consequently, decide whether to ignore or delete them. The consequences of this decision could lead to expanding the boundaries of active monitoring by online platforms with consequences on the right to freedom of expression,[35] namely a global "assault on speech".[36]

Nonetheless, the primary problem is still unsolved: the shortage of control mechanisms for users in the process of content moderation such as, for example, access to redress mechanism against social media' decision. Although the AG Spuznar had suggested the need for a mechanism for controlling the content moderation activity also in line with the need to protect the freedom of expression referred to in Art. 11 of the Charter of Fundamental Rights,[37] there is no sign of this argument when looking at the Facebook decision. This lack is not surprising for two reasons. The recognition of new rights would have led the CJEU to play the role of the European legislator, thus, extending the protection of freedom of expression online horizontally, as occurred for the protection of personal data in the *Google Spain* case.

Furthermore, the absence of procedural safeguards is also be linked to a more general

EU Internet Law & Policy Blog, 4 October 2019.

[33] A. Stariano, *Facebook Can Be Forced to Delete Content Worldwide, E.U.'s Top Court Rules*, in *The New York Times*, 3 October 2019

[34] K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in *Harvard Law Review*, 131, 2018, 1598 ss.

[35] D. Keller, *Dolphins in the Net: Internet Content Filters and the Advocate General's Glawischnig-Piesczek v. Facebook Ireland Opinion*, Stanford Center for Internet and Society, 4 September 2019.

[36] J. Daskal – K. Klonick, *When a Politician Is Called a 'Lousy Traitor,' Should Facebook Censor It?*, in *The New York Times*, 27 June 2019. See, instead, A.K. Woods, *The CJEU Facebook Ruling: How Bad Is It, Really?*, Lawfare, 4 October 2019.

[37] Opinion of Advocate General in C-18/18, cit., § 65.

issue. In particular, in the Courts' reasoning, there is no reference to the impact that a system of moderation based on identical or equivalent content would have not only on the balance between the victims' honour and the freedom of economic initiative of the platform but also on the fundamental rights of users. More specifically, the rise of complexity in content moderation could undermine users' freedom of expression due to the risk of collateral censorship, algorithmic biases and surveillance over speech. Besides, the users' protection of privacy and personal data could also be involved due to the increase in the processing of data of other users to detect identical and equivalent content. It is no by chance that the AG Spuznar had argued in its conclusions that the extension of the obligation to remove equivalent content not only of the applicant but also of third parties would require "the monitoring of all the information disseminated via a social network platform".[38] As explained by Woods, "the statement of the Court that searching for an individual item of content does not constitute general monitoring does not address the fact that such a search would presumably involve search all content held".[39]

Likewise, the CJEU made no reference to a time limit applicable to national orders of removal and block. The AG Spuznar had proposed to provide a time limit even if he recognised that the case in question concerns an obligation imposed in the context an obligation imposed in the context of an interlocutory order, which is effective until the proceedings are definitively closed. Therefore, such an obligation imposed on a host provider is, by its nature, limited in time.[40] However, it cannot be excluded that platforms could be subject to comply with these obligations indefinitely to continue assessing the relevance of any circumstance that could concern identical and equivalent content. In fact, this ruling has the potential to open the doors to proactive behaviours on the part of platforms consisting of monitoring content not to incur responsibility for additional identical and equivalent information hosted in their digital spaces.

With regard to the second strand of the decision, the first question that deserves to be underlined is the absence of references to which rules of international law the Member States should refer to assess the territorial scope of removal orders. Some perspectives on this point can be found in the decision of the CJEU in the Google case. In this case, the CJEU expressly refers to the potential contrast of a global delisting order with the protection of rights at an international level. Therefore, national competent authorities can indeed strike a fair balance between individuals' right to privacy and data protection with the right to freedom of information. However, the different protection of freedom of expression at a global level would limit the application of the balancing results. The AG Spuznar reaches the same conclusion in the Facebook case, explaining that, although EU law leaves Member States free to extend the territorial scope of their injunctions outside the territory of the Union, national courts

[38] *Ivi,* § 73.

[39] L. Woods, *Facebook's Liability for Defamatory Posts: The CJEU Interprets the E-Commerce Directive*, EU Law Analysis, 7 October 2019.

[40] Opinion of Advocate General in C-18/18, cit., § 60.

should limit their powers to comply with the principle of international comity.[41]
This trend towards local removal is based not only on the *status quo* of EU law at the time of the decisions but also on the effects that a general extension of global remove can produce in the field of content and data. As observed by the AG Spuznar, a worldwide de-referencing obligation could initiate a «race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale».[42] In other words, the CJEU's legitimacy could start a process of cross-fertilisation, thus, leading other countries to extend their removal order on a global scale. This could be particularly problematic when looking at authoritarian countries which could exploit this decision to extend their orders.[43]
Moreover, in the Google decision, the CJEU explained that the limit for global removal also comes from the lack of intention to confer an extraterritorial scope to right to erasure established by the GDPR.[44] The lack of cooperation mechanisms between competent authorities extending outside the territory of the Union would confirm this argument. Nevertheless, by supporting this position, the Luxembourg Court, however, did not consider that, more generally, the GDPR establishes a broad territorial of application covering processing activities related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behaviour as far as their behaviour takes place within the Union.[45]
Nonetheless, it is worth underlining that the Union has not closed the doors to the possibility of extending the territorial scope of removal orders beyond EU borders. At first glance, the Luxembourg judges seem to express at an opposite view in the two cases regarding the territorial scope of national orders. On the one hand, in the Google case, the CJEU states that EU law does not require search engines to carry out the delisting of information and links on a global scale. In the Facebook case, on the other hand, the CJEU explains that there are no obstacles to global removal, but also it leaves the evaluation to the Member States. Although the two judgments may seem opposite, they lead to the same result, namely that EU law does not either impose or preclude national measures whose scope extends worldwide. This is a decision which rests with Member States which are competent to assess their compliance with international obligations. Art. 18 of the e-Commerce Directive does not provide a specific territorial scope of application and the CJEU has not gone further. Otherwise, «it would have trespassed within the competencies of Member States, which under EU law retain primary legislative power on criminal law matters».[46]
Besides, the reasons for this different approach can be attributed to the different de-

[41] *Ivi,* § 100.

[42] *Ivi,* § 61.

[43] D.B. Svantesson, *Bad News for the Internet as Europe's Top Court Opens the Door for Global Content Blocking Order*s, LinkedIn, 3 October 2019.

[44] C-507/17, cit., § 62.

[45] GDPR, Art. 3(2).

[46] E. Brogi – M. Maroni, *Eva Glawischnig-Piesczek v Facebook Ireland Limited: A New Layer of Neutrality*, CMPF, 7 October 2010.

gree of harmonisation of the protection of personal data and defamation as observed by the AG Spuznar.[47] Therefore, it is not just an issue concerning public international law but also private international law contributes to influencing the territorial scope of removal orders.[48]

Despite the relevance of the aforementioned point, leaving Member States free to determine when a national order should be applied globally could lead to different national approaches which would fragment harmonisation goals. This is particularly relevant in the framework of the GDPR since it provides a new common framework for Member States in the field of data. Indeed, while the content framework still relies on the e-Commerce Directive leaving margins of discretion to Member States, this approach in the field of data is more problematic. On the one hand, the GDPR extends its scope of application to ensure a high degree of protection of fundamental rights of the data subjects. On the other hand, the GDPR leaves Member State to implement open clauses that could undermine its constitutional scope. This is particularly evident when focusing on derogations that Member States can introduce with regard to processing for journalistic purposes and artistic or literary expression. As Zalnieriute explains,

«[b]y creating the potential for national data protection authorities to apply stronger protections than those afforded by the GDPR, this decision could be seen as another brick in the "data privacy wall" which the CJEU has built to protect EU citizens».[49]

Furthermore, even in this case, the CJEU has not focused on the peculiarities of platforms' activities and the consequences of these decisions on the governance of freedom of expression in the digital space. In the Facebook case, a local removal order would not eliminate the possibility of accessing the same content – identical or equivalent – through the use of other technological systems or outside the geographical boundaries envisaged by the removal order. This problem is particularly relevant in the Google case since it is possible to access different Google domain names around the world easily. The interest in the protection of reputation could also require an extension beyond the borders of the Union to avoid relying just on partial or ineffective remedies. It is indeed the CJEU which recognised that access to the referencing of a link referring to information regarding a person in the EU is likely to have «immediate and substantial effects on the person».[50] Therefore, even if this statement is just one side of the balancing activity with the protection of international law on the other side, it leads to contradictory results frustrating data subjects' right to be forgotten due to the potential access to search engines' domain names. Furthermore, to comply with geographical limits, geo-blocking and other technical measures would require an additional effort for platforms, thus, increasing the risk of censorship on a global scale and create a technological barrier for small-medium platforms.

47 Opinion Advocate General in C-18/18, cit., § 79.

48 P. Cavaliere, *Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations*, in *European Data Protection Law*, 4, 2019, 573 ss., 577.

49 M. Zalnieriute, *Google LLC v. Commission Nationale de l'Informatique et des Libertés (CNIL)*, in *American Journal of International Law,* 114(2), 2020, forthcoming.

50 C-507/17, cit., § 57.

5. Paths of Convergence and Divergence

The two decisions share points of convergence and divergence. On the one hand, both cases deal with the activities of two of the most relevant online platforms like Facebook and Google and the territorial scope of judicial and administrative orders of removal. From a different perspective, the close time frame of these two decisions outlines an autumn that has been defined "hot" for the protection of fundamental rights online and the challenges of constitutionalism.[51] On the other hand, the decision underlined how the legal regime of data and content are based on different pillars and the differences in these two decisions show this constitutional distinction which, however, is going to converge in the algorithmic society.[52]

These considerations do not exhaust either the questions left unsolved by these decisions or leads to solutions in the field of content and data. The field of content and data has shown to be based on different set of rules that does not only concern the applicable legal regime but also the potential territorial scope of application. Nonetheless, from a broader perspective, unlike other decisions in the past in the field of data protection such as *Google Spain* or *Schrems*,[53] the CJEU has adopted a more cautious approach to issues relating to freedom of expression and data protection in the digital space. On the one hand, such a restrictive approach seems to undermine a constitutional framework for the protection of fundamental rights in Europe that focuses not only on the territorial dimension but on respect for the rights and freedoms of the individual in a transnational digital context. The approach of the Union provides clearer rules on the scope of application of removal obligations in the field of content and data even if the challenges raised by these decisions for the effective protection of fundamental rights online are still concerning.

[51] O. Pollicino, *L' "autunno caldo'" della corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *federalismi.it*, 16 October 2019.

[52] G. De Gregorio, *The e-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?,* Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2019/36.

[53] CJEU, C-362/14, *Schrems* (2015).