

**FREEDOM OF EXPRESSION ON THE INTERNET - CASE 18/18 EVA
GLAWISCHNIG-PIESCZEK V FACEBOOK IRELAND LIMITED**

Katarina KNOL RADOJA

E-Mail: kknol@pravos.hr

Assistant Professor, Phd.

Faculty of Law, Josip Juraj Strossmayer University of Osijek
Stjepana Radića 13, Osijek
Croatia

Abstract

The democratic world has invested much effort to achieve the conditions for full freedom of expression of the media, but still with that freedom other human rights and freedoms must be respected. What if the publication of information that is incorrect has the potential to cause some sort of damage or harm to an individual or the public? The problem of misinformation then raises the issue of legal interference and regulation. The vast problem today is that any posting on social networks can be spread and be shared with high speed, and the mere fact that a court ordered the removal of an original defamatory statement will often have no positive effects for the injured party since the information has been and will continue to be shared on the profiles of other users. In its recent decision in Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, the Court of the European Union sets out rules for imposing an obligation on an information society service provider, ie. a social network, to delete and /or block access to identical and equivalent posts and links previously declared to be illegal without breach of Article 15 of the E-Commerce Directive. This is a significant judgment with global implications. Before this judgement, at the request of a national court, posted content in the requesting state has been removed, but after this judgement, the force of the law can compel the controversial content in question to be removed from all servers around the world. An analysis of the judgment leads to the conclusion that the confirmation that a national court is entitled to request the removal of posts on a worldwide basis points to the fact that the Court of the European Union understands the limitations and unfairness of solutions when social networks restrict access to offensive and defamatory content only for IP addresses from a specific country. This decision extends the reach of EU legislation concerning the internet outside its borders. However, a high level of caution should be maintained so that excessive scrutiny of published content does not violate the freedom of expression.

Key words: *personal rights, freedom of expression, territorial scope, equivalent content*

1. Introduction

Personal rights and freedom of expression may conflict, or appear as a restriction on one another. The right to expression can be seen as coming into conflict with the honor, reputation, privacy or identity of a natural or legal person. Reporting that goes beyond the information needs of the public can penetrate the protected areas of human dignity. Resolving conflicts of interest between the personal rights of the natural and legal persons on the one side and the freedom of expression on the other is the subject of interest of many domestic and foreign scientists. What makes this area particularly distinctive is its interdisciplinary nature so that not only scholars¹ in the field of media and other branches of law are concerned with this topic, but it is also the subject of interest of communication scholars, ethicists and other experts (Knol Radoja, 2015, p. 92).

Compared to other media, the internet is unscrupulous and advantageous in the amount of untested sensationalist information, due to the commercialization of the market (Ružić, 2008, p. 104). A factor that has further facilitated the dissemination of information on the internet is the emergence and popularization of social networks. The possibility of anonymity on social networks gives individuals a sense that they can avoid possible consequences of their actions and therefore have greater power. Thus encouraged, through various social networks, they often spread defamatory and discriminatory information (see more in MunivranaVajda, Šurina Marton, 2016, p. 453). In addition, internet content is largely permanent, allowing victims of cyberbullying² and invasion of privacy to be continually harmed. In the past, the effects of printed defamation have disappeared over time as newspapers and magazines have been sent to waste bins or to piles in the library. However, with the internet, defamation, once it is published, offensive content rarely loses its validity (Johnson, Johnson, Tweed, Smolla, 2019, p. 10).

In recent months, numerous judgments have been delivered regarding the control of information on the internet. The most recent was judgment of the Court of the European Union (hereinafter: CJEU, or Court) in *Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited* that was handed down on 3 October 2019. This judgment concerned the impact of the 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 (hereinafter: E-Commerce Directive), specifically the prohibition on general monitoring found in Article 15 of that Directive.

The aim of this paper is to analyze the aforementioned judgment. *Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited*

¹ The references cited in this paper, which were originally written in Croatian, were translated by the author of this paper.

² Cyberbullying, also known as online bullying, is a form of harassment using electronic means.

stemmed from a defamatory comment posted on Facebook about Austrian politician Eva Glawischnig-Piesczek, which courts in that state said had harmed her reputation. Following the Court ruling, Facebook and similar websites, were ordered to remove illegal posts around the world. On this basis, the territorial reach of user protection measures emerges as an issue. Moreover, the social network will also have to look for similar examples of illegal content and remove them, instead of waiting for individual applications.

This judgment seeks to strike a balance between the right to protect the reputation and privacy of information society services (OTT services³), OTT service users, especially the right of certain users to protect themselves from offensive and defamatory content disseminated through the internet (above all social networks, as a type of OTT service providers) and the right of OTT service providers to protect against disproportionate claims. Also, by reducing the number of claims, the courts are relieved of number of similar cases. It is a significant judgment with global implications, though on the other hand, it raises critical issues of freedom of expression. We must expect far-reaching consequences on the free expression and access to information for both internet users and internet intermediaries. In addition, too much control could jeopardize the neutral status of intermediary providers.

2. Freedom of expression

The Universal Declaration of Human Rights (1948), the Charter of Fundamental Rights of the European Union (2010) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) are just some of the international conventions that protect and guarantee freedom of expression as one of the fundamental human rights. Like all guaranteed freedoms, freedom of expression has been understood as the ability to do all that does no harm to others, which means that the boundaries of freedoms and natural rights are determined by the boundaries of those same rights held by other people (Vodinelić, 2003, p. 13). It is a fundamental legal principle that one right or freedom must not endanger or abolish another right or freedom, but that every right and freedom is to a certain extent, limited in order not to jeopardize the other. However, there is no regulation that clearly defines where freedom of expression ends and when such expression begins to be considered inadmissible. Thus, in practice, the boundaries of personal rights will often vary from case to case, and thus will be left to the courts in individual cases (Stratford, 2002, p. 17).

It is also a question if the freedom of expression is associated with a sufficient level of professional standards and accountability. In some cases, it is objective and professional reporting, but in others, it is either manipulation

³ OTT services can be defined as services provided through networks of electronic communications operators, which may be chargeable or free of charge to users, and which are in direct competition with services provided by electronic communications operators (such as social networks).

of facts or falsehoods are published that can consequently destroy one's family life and social reputation (Skoko, Bajš, 2007, p. 93). Although we can say that freedom of expression is certainly one of the greatest achievements of democratic societies, the fact is that it cannot be itself sufficient for that societies to function balanced. And although it is extremely important for the realization of fundamental human rights and freedoms, the exercise of these human rights and freedoms also involves duties and responsibilities and thus may be limited in certain situations (see more in Knol Radoja, 2015, p. 98). There is no freedom of expression that is absolute.

According to Article 11 of the EU Charter of Fundamental Rights, everyone has the right to freedom of expression. This right "shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The freedom and pluralism of the media shall be respected." However, Article 52/1 stipulates that "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

Also, Article 10 of the European Convention protects freedom of expression. This right includes freedom of opinion and freedom to receive and impart information without interference by public authority despite frontiers. However, paragraph 2 of the same Article also provides that the exercise of these freedoms, may be subject to some restrictions as are prescribed by law and are necessary in a democratic society (for example in the interests of national security, for the protection of health or morals, of the reputation or rights of others, for preventing the disclosure of information received in confidence etc.). These exceptions are followed by the European Court of Human Rights by applying a three-part test in each particular case. The European Court of Human Rights first examines whether the restriction applied in a particular case was prescribed by law (the principle of legality), whether such a restriction was prescribed in order to protect a legitimate aim (the principle of legitimacy) and whether these restrictions were necessary for a democratic society (necessity principle) (Alaburić, 2002, p. 31). Although the list is broad and extensive, it does not mean that the given reasons can justify any interference with this right. However, a restriction incompatible with one of these categories will not be allowed and will constitute a violation of Article 10 of the European Convention.

For the purpose of this paper, the most important restriction of freedom of expression, as one of the legitimate aims, is the restriction to protect the reputation or rights of others. However, guaranteeing full advantage to one or the other is neither a fair nor an acceptable solution, since there is no compelling reason to favor one of the fundamental rights over the other. If there was a preference for one of two equally important fundamental rights, it would inevitably lead to an unacceptable disregard for the other

right. Instead, if there were two equally important rights, it would be better that there be additional criteria that would dictate the order depending on the relevant circumstances of each individual case (Koziol, 2005a, p. 685). How much the protection of freedom of expression is worthy, depends on whether or not the statement of facts in question is true. Koziol points out, considering the purpose of freedom of expression and the related right to information, only the interest of accurate and proper information that is worthy of protection. This will not, however, mean that only absolutely true statements may be disseminated, but that the information will need to be properly verified prior to its publication (Koziol, 2005, p. 261). However, the truth may be the determining criterion in the case of a statement of fact, since only such statements can be objectively examined. When it comes to expressing opinions (value judgments), it is a strong subjective component, which can therefore hardly be qualified as objectively accurate or inaccurate. Uncensored expression of opinion reflects the fundamental constitutional guarantee of free speech. However, interest in protecting the expression of opinion should not exist if it is offensive. Such an opinion will affect the personal rights of the affected person (Koziol, 2005a, p. 686).

3. Legal framework applicable to information society services in EU

With the advent of the internet, the legal problems of restrictions on freedom of expression have been raised to a higher level. It is no longer just about the press release of official media and journalists, it is about the publication of every post by any individual with access to the network. In the "normal" world, the general legal principle of deciding the eventual liability for published information is territorial, determined by the laws of a particular country applied within its borders. However, given that the internet knows no national borders, published information can be accessed by anyone from anywhere in the world.

There are a number of questions raised regarding the proper application of the rules on the protection of different personality rights in the digital environment, from the substantive and territorial application of the relevant EU framework to the substantive and procedural details regarding the role, obligations, and responsibilities of relevant actors in the publication of information on online social networks.

The legal framework applicable to OTT services, users and national courts in the EU is primarily determined by Articles 14, 15, and 18 of the E-Commerce Directive. In the EU, in addition to users who are, under certain circumstances primarily responsible, OTT service providers, such as Facebook, are responsible for being aware of any illegal activity (secondary liability) (Sartor, 2017, p. 4). In accordance with Article 14 of the E-Commerce Directive, Member States must ensure that the service provider is not responsible for the information it stores, under "condition that the provider does not have actual knowledge of illegal activity... and is not aware of facts or circumstances from which the illegal activity or information is apparent; or the provider, upon obtaining such knowledge or awareness, acts

expeditiously to remove or to disable access to the information”(Article 14 of the E-Commerce Directive).

However, the legal framework does not clearly define the scope of OTT providers' obligations on the internet. In accordance with Article 15/1. E-commerce Directive EU Member States may not impose on intermediary service providers a general duty to monitor information that they transmit or store. From the provision, it follows that the prohibition does not apply to monitor obligations in a particular case, nor does it affect the obligations imposed under national law. In this regard, considerable emphasis has been placed on how much this will depend on legislation, which will ultimately require the courts to take into account the proportionality and balance between fundamental rights (Harvey, 2019, p. 837). Also, service providers can, on their own initiative, monitor activities on their platforms to maintain a civilized environment. However, voluntary monitoring can also prove detrimental. Too much control could jeopardize the neutral status of service providers (Kuczerawy, 2019, p. 142).

The Directive does allow the States to require service providers to detect and prevent certain types of unlawful acts provided for under national law. However, the Directive does not specify what exactly such obligations entail. As a result, the boundary between the duty of care and general supervision is not clear (see more in Valcke, Kuczerawy, Ombelet, 2016). Therefore, prior to the judgment of the CJEU in *Case C-18/18 Eva Glawischnig-Piesczek v. Facebook Ireland Limited* (hereinafter: Decision) it was not clear to what extent OTT service providers must delete postings and whether it must delete the post just in the state where the lawsuit was filed or worldwide.

4. *Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited*

Eva Glawischnig-Piesczek was a Member of Parliament in the National Council of Austria, while Facebook Ireland manages Facebook for users located outside the US and Canada. The case is about a Facebook user who shared an article on Glawischnig-Piesczek which was accompanied by his offensive and defamatory comment. He posted the article and commentary on the article publicly, not just within his Facebook friends network. Although in July 2016 Glawischnig-Piesczek requested that Facebook Ireland remove the link, Facebook Ireland did not do so. Therefore, Glawischnig-Piesczek filed a lawsuit in the Commercial Court in Vienna, which ordered Facebook Ireland, with immediate effect and until the proceedings relating to the action for a prohibitory injunction have been finally concluded, to stop and desist publishing and/or disseminating of the link. Facebook Ireland did it, but only for the territory of Austria. The Vienna High Court upheld the measure at first instance on appeal. However, it also opined that the spread of allegations of equivalent content had to stop only in relation to those learned about in the main proceeding by the applicant, third parties or otherwise. Both parties of the main proceeding brought an appeal before the Austrian Supreme Court.

Having been requested to give a ruling whether the stop and desist injunction made against a host provider which managed a social network with numerous users may also be extended to publications with identical wording and/or having equivalent content of which it is unaware, the Supreme Court articulates that, in line with its case-law, such an obligation must be taken into account to be proportionate where the host provider already knew that the interests of the person concerned had been injured at least one time as a result of a user's post and the chance that other violations may be committed have thus shown (Decision, para. 19). However, considering that the dispute in the main proceedings raised questions of the interpretation of EU law, the Supreme Court decided to stay the proceedings and refer the preliminary questions to the CJEU on the interpretation of Article 15/1 of the E-Commerce Directive.

The Court began its analysis by clarifying that immunity from a claim under Article 14 of the Directive is not general immunity from all legal liability. In particular, the national authorities are competent to require a host to revoke access/remove illegal information (Decision, para. 23., 24.). The Court also emphasized that Article 18 of the E-Commerce Directive obliges Member States to provide adequate judicial actions to address illegal content (Decision, para. 26.).

a. Territorial scope

The first thing the court in the analyzed judgment needed to clarify was the appropriate geographical scope of the order passed by the competent court. In other words, can a court of a Member State order an OTT provider (social network) to extend the effects of such an order worldwide, ie. not to keep them within the borders of the Member State and / or the EU?

This question is important because of Facebook Ireland initially, at the request of an Austrian court, limited access to the defamatory post exclusively on the territory of Austria, or from users accessing from Austrian IP addresses. The usefulness of such a solution is questionable, since Facebook is not a national Austrian social network, so users from other countries have access to it. Also, restricting access only at the national level can be very easily circumvented using widely available Virtual private network (VPN) services.

To answer the question, the Court stated that, as is seen in Article 18/1, the E-Commerce Directive does not provide for any restriction, including territorial, of the scope of the measures that the Member States may adopt in accordance with this Directive. Consequently, the E-Commerce Directive does not preclude the above-mentioned ordering measures from producing effects worldwide (Decision, para. 49., 50). Apropos, if the law of a Member State allows a safeguard measure to have an extraterritorial scope, no provision of the E-Commerce Directive prevents a Member State's court from ordering an OTT service provider to remove data covered by an injunction in several states and even globally. However, it is important to emphasize that neither does it say that the injunction should have an extraterritorial effect.

In other words, the national rules of civil law and civil procedure of a particular Member State apply in the case of a violation of personal rights and safeguard measures. However, in his opinion, AG Szpunar notes that the effectiveness of such an order depends to a large extent on the framework of the relevant international law, in particular on the rules for the recognition and enforcement of decisions or judgments of a foreign court (international civil proceedings) (Opinion of AG Szpunar, para. 92).

In its decision, the Court emphasized the need to ensure the consistency of European Union rules with the rules applicable at the international level and that it is on the Member States to ensure that the measures they enact which produce effects at world level duly take into account the latter rules (Decision, para. 51, 52). In doing so, the provisions of the Regulation (EU) (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters,⁴ should also be taken into account, though one should keep in mind that a court with jurisdiction originated in EU law (for more on jurisdiction: Knol Radoja, 2018., Tagaras, 2015., ch. 10.; Bogdan, 2011., Revolidis, 2017) does not have unrestrained universal jurisdiction just because it applies national law (Svantesson, 2019, p. 398, 400). In his Opinion, AG Szpunar emphasized that a court, in such a case, should adopt an approach of self-limitation and limit the extraterritorial effects of its injunctions concerning harm to personal rights. The fulfillment of a removal obligation should not go above what is vital to achieve the protection of the damaged individual (Opinion of AG Szpunar, para. 100).

b. Equivalent content

In this judgment, the CJEU also focused extensively on the limitation of the power of national courts to impose obligations on service providers concerning the blocking and removal of illegal content. The Court ruled that the national court could order the service provider to block or remove stored data identical to content previously affirmed illegal, regardless of who requested the storage of that information (Decision, para. 53). In other words, the Court argued that such a prohibition was permissible and that it was part of the special supervision allowed in recital 47 of the E-Commerce Directive. The Court also stated that the E-Commerce Directive does not prohibit the issuing of a restraining order for information with equivalent content in

⁴ Most of the concerns regarding jurisdiction over civil and commercial disputes at EU level have been resolved by Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 012 , 16/01/2001 P. 0001 - 0023.) which was subsequently replaced by the Regulation (EU) (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1–32.).

statements affirmed illegal. This solution is explained by the fact that the illegality of the data stems from its content, not the use of certain expressions in a particular way (Decision, para. 53).

It may be noted that a request to remove similar content is not a new concept. Similar provisions have been formulated in cases of infringement of intellectual property rights so that the infringer cannot easily circumvent the court order by making minor changes in his product. However, unlike the situation in cases of personal rights violations, there are specific legal reasons that justify the issuance of such broad prohibitions or orders. For example, according to the Article 9/2. Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trademark, the trademark owner has the right to prevent any unauthorized third parties from using any sign identical or similar to their sign (under condition that the other requirements set out in the provision are met).

Enforcement of the prohibition the disclosure of equivalent information must allow access the information expressed in a slightly different way, but in essence conveying the same message. The judgment acknowledges the real nature of posts on social networks, and goes beyond the grammatical interpretation of the "equivalent" of posts. The Court stated that any statement on social networks can be spread and shared at high speed, and the mere fact that a court ordered the removal of an original defamatory statement will often have almost no positive effects for the injured party, since often such a publication with a minimal grammatical but no substantive changes would be further shared on profiles of other social network users (Decision, para. 36). In these circumstances, to prevent any new harm, the competent court may require the blocking of access or removal of information which content is identical to those previously affirmed illegal. In view of the identical content of the information in question, an injunction issued for this purpose cannot be considered as establishing an obligation of general supervision within the meaning of Article 15/1. of E-Commerce Directive (Decision, para. 37). Furthermore, for an injunction to end and prevent an unlawful act to effectively achieve its objectives, that injunction must be able to extend to information the content which, although basically conveying the same message, is formulated in a slightly different way. It is important that the same information includes specific elements duly identified by the author of the injunction, such as the name of the person to whom the violation was previously identified, the circumstances in which the violation was determined, and the content equivalent to the content affirmed illegal (Decision, para. 41, 45). Otherwise, the effects of such an injunction could easily be bypassed by storing messages that are slightly different, which could lead to the person concerned having to initiate many new court procedures to protect himself. In doing so, what is crucial to note is that the Court stated that differences in the formulation of content of the same type as content declared illegal should not be such as to compel the OTT service provider to evaluate the content independently (Decision, para. 45). That is, the OTT service provider may be ordered to monitor or seek equivalent content in breach of

the injunction, but at the same time should not be instructed to make an independent assessment of the legal or illegal nature of that content.

The CJEU therefore established an obligation for the national court to indicate in a sufficiently specific manner to the OTT provider (social network) the criteria on which it will search and remove posts and links that are "equivalent" to a publication that was declared illegal. These criteria are very important and, but since they are not available, the social network would be obliged to monitor the information they transmit or store, which is opposite to Article 15/1. E-Commerce Directive.

In his Opinion, AG Szpunar also expressed his concern about the monitoring of equivalent content. He stated that not only would the role of a service provider operating overall monitoring no longer be impartial, in the sense that it would not be just technical, passive and automatic, but that service provider, by performing a kind of censorship, would turn into an active contributor to that platform (Opinion of AG Szpunar, para. 73). How supervision will be exercised remains unclear. The only explanation could be that during an internet search for one thing, other things are not look at, which could be achieved if the search was automated (Vazquez, 2020, p. 73).

5. Case Facebook and cases against Google – comparison

The CJEU judgment in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* of 13 May 2014. (hereinafter: *Google Spain*), although not made on the issue of the protection of the right to the honor and reputation of the individual, rather on the protection of personal data, it is in many ways comparable to the analyzed judgment. The case concerns the right of individuals to request, under certain conditions, that the internet search provider (search engine operator) cease to include their personal information, ie. links to third party websites with this information in search results by their name even when it is about legally posted content or content that has not been removed from the source page. Although it is often called "right to be forgotten judgment", it is a bit of a misleading name since the information in question will not be deleted, ie. it remains on the internet, and remains accessible to search engine users if they use some other search criteria. Nevertheless, at least at first, the judgment was considered controversial. The main reason for this was the divided public reaction to the emphasis on the fundamental rights of individuals in Europe to privacy and protection of personal data in relation to freedom of expression and information on the internet (Rufer, 2015, p. 37). However, based on this judgment, the content at issue remained in its original place on the web and could be found by searching on terms other than the name of the person concerned. Gumzej, for example, states that if a respondent's request to remove a link to an old story about him in a student journal is accepted, that story can still be found, for example, by searching the names of other persons mentioned in that story or the faculty in question (Gumzej, 2016, p. 187). This was the shortcoming the CJEU was attempting to overcome in the analyzed judgment against

Facebook. By establishing an injunction on the publication of equivalent content, the possibility of circumventing the prohibition of access to published illegal content should be limited to the maximum.

In addition, the *Google Spain* judgment also interprets the application of EU rules on the protection of personal data to a web browser provider located outside the European territory (eg. the United States of America) and establishes its responsibility for the removal of certain personal data of individuals in Europe from his search results. Under the Directive⁵ that was applicable at that time, the applicable law is the law of an EU Member State where the controller of the personal data collection office was established if the processing of personal data was carried out in the perspective of the activities of that establishment. The law of an EU Member State will be relevant even when the controller of the personal data collection is not established on its territory if its domestic law is applied under public international law. If the controller does not have an establishment in the EU but the equipment used for the processing of personal data is in the territory of one of the EU Member States, then that Member State's law will be applicable (Article 4 of Directive 95/46). In a particular case, in accordance with these provisions, the CJEU identified as relevant to the Spanish personal data protection law in which the Directive was implemented. He determined this on the basis of the applicable law of the EU Member State where the controller of the collection is established if the “processing of personal data is carried out in the context of the activities of that establishment.” He considered that the above also encompassed a situation where a non-EU search engine operator (Google Inc., USA) establishes a subsidiary or a specific subsidiary in a Member State (Google Spain, Spain) for the purpose of “promotion and sale of advertising space” offered by that search engine which targeted its activity towards residents of that Member State (*Google Spain*, para. 45, 100).

Based on the above, “the decision institutes the foundations for extraterritorial regulation of relevant activities of internet actors providing services on the European market, out of which a considerable number with a prevailing share on that market is not founded on the territory of EU” (Gumzej, 2016, p. 171).

In another significant case against Google, in the judgment in the case *Google Inc. v. CNIL* from 24 September 2019. (herein after: *Google v CNIL*) concerns the interpretation of Regulation (EU) 2016/679 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 (GDPR) looking at the obligations of search engines. The judgment was delivered just a few days before the judgment against Facebook. It is significant to emphasize that the CJEU explicitly placed restrictions on the territorial scope of the individual's right to de-reference. The Court ruled that there was no obligation under EU

⁵Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/31.

law for Google to globally exercise the European right to be forgotten (*Google v CNIL*, para. 64, 66). The decision made it clear that while EU residents have a legal right "to be forgotten", that right applies only inside the borders of the Member States.

Simply put, this indicates that Google only has to remove links to personal information from EU-wide online searches. However, it did not rule out the probability that some cases may rationalize a global de-referencing (*Google v CNIL*, para 72.; Samonte, 2019). Nevertheless, even before the ruling itself, the doctrine emphasized that this would involve censorship and the global imposition of rights in Europe, which can become a dangerous precedent in the context of internet regulation (Fleischer, 2015). Besides, in the case of *Google v CNIL*, the Court explicitly noted that the courts must weigh the rival interests of the data subjects and the right to freedom of information of others (*Google v CNIL*, para 72.).

It is evident that in *Eva Glawischnig-Piesczek v Facebook Ireland Limited* the balancing is different. The Court notes to some extent the need for the provider not to be unduly burdened (*arg. ex. Decision* para. 46). But, there is no explicit mention of the existence of other rights: the right of the host to do the job and the rights of those who publish the material and those who wish to obtain it, both aspects of freedom of expression. To some extent, the issue of these rights will be raised before national courts, which will be the bodies that will implement this balance within their national frameworks and EU law.

Unlike in *Google v CNIL*, The Court has neither developed questions that need to be considered, nor any explicit acknowledgment that the balance between the right to privacy (including protection of reputation) and freedom of expression varies between states. What can be considered a legitimate protection of privacy in one state could be a violation of free speech in another. So, even though these issues in this case were not direct concern of the Court, it is surprising that they were not directly discussed (Woods, 2019).

6. Conclusion

In the modern information society, with the advent of new communication tools and technologies, almost unlimited possibilities for the violation of citizens' personal rights are opening up. The spread of freedom of expression over the endless internet websites has raised the issue to an even greater level. In these circumstances, the fundamental question is how to regulate the relationship of the two conflicting human rights, respectively, how to secure the right of citizens to disseminate and receive information, while at the same time protecting their personal rights. By widening the reach of information published in the media, the detrimental consequences of false posts are becoming more evident, so an effective legal response is needed.

Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited can be considered as a major case concerning the freedom of expression on the internet to come before the Court of the European Union and which will undoubtedly affect national judicial decisions of EU Member

States and beyond. In this judgment, the Court imposed additional obligations on certain OTT service providers, relating to the protection of users against offensive and defamatory content on social networks. Also, particular emphasis should be placed on extending the obligation to delete such content to cases where the content is further shared on the social network (even globally) when the form is slightly modified, but the content remains the same. In addition to greater protect users' personal rights, since social networks will have to look for similar examples of illegal content and to remove them, rather than waiting for individual claims, this decision could have the effect of unburdening the judiciary. Confirming that a national court has the right to seek the removal of content on a worldwide basis points to the fact that the Court understands the limitations and unfairness of the solutions when social networks restrict access to offensive and defamatory content only for IP addresses from a specific country.

However, the judgment also leaves some questions unanswered. Why, in two judgments delivered only a few days apart, the judgment in the case of *Google v CNIL* and the analyzed judgment, the Court has a completely different view of the territorial scope. It appears that with regard to the geographic scope of injunctions, injunctions issued in respect of national rights that have not been harmonized at the EU level should be only taken into account in exceptional cases.

The Court stated three elements that should form the injunction: 1) the name of the person to whom the violation relates, 2) the circumstances in which the violation was identified and 3) differences in formulation. However, it does not establish sufficiently clear and specific guidelines on the basis of which the social network or national court will determine what is considered to be equivalent content, and how the social network will determine such equivalent content, especially since it emphasizes that differences in the formulation of such content should not force the OTT providers to independently rate this content. Thus, instead of prescribing specific parameters that are to be considered equivalent content, the Court provides a general provision with a very broad scope. The social network may be forced to judge what exactly the equivalent content is and what is explicitly forbidden. Although requesting a social network to find this other content cannot be considered as introducing a monitoring obligation forbidden by Article 15 of the E-Commerce Directive, listed criteria are to some extent contradictory, because the service provider will only understand whether to carry out this assessment after the performed surveillance, which then cannot be undone. The elements listed in the injunction may contain subtle changes and require additional analysis and a real understanding of the context of the content.

Furthermore, the Court did not mention the period during which such an injunction would be enforceable. For example, as the public loses interest over time, such injunctions may become disproportionate and have a discouraging effect on freedom of expression. Since an injunction might cover future identical and equivalent infringements, the enforceability of the

injunction should always be limited in time. Additional ambiguity arises with the possibility of an obligation to remove offensive and defamatory content worldwide. The Court obliges the Member States to ensure in such situations that the rules of the Union are consistent with those applicable at the international level. However, it does not specify exactly which international rules and conventions it refers to, and to some extent leaves the Member States in suspense.

Finally, what if the posts were transmitted satirically or in audiovisual form? The provider will have to balance the freedom of speech and expression of its users and the injunction. However, as has been pointed out many times before, the provider may not be obliged to carry out an independent assessment, so it may end up in a rather unenviable position. Taking all of the above into account, it can be concluded that it is currently difficult to imagine that this obligation would not constitute a general monitoring obligation. The implementation of some measures may sometimes turn into censorship. Besides, although the fact of acting upon a court order protects the service provider from liability, the tendency to remove allegedly illegal content can have significant consequences for individuals' ability to access and share content online, and may discourage and adversely affect the exercise of free speech.

References

Books and articles

- Alaburić, V. (2002). Sloboda izražavanja u praksi Europskog suda za ljudska prava [Freedom of expression in the case law of the European Court of Human Rights]. Zagreb, Narodne novine
- Bogdan, M. (2011). Defamation on the internet, forum delicti and the E-Commerce Directive: some comments on the ECJ judgment in the eDate case. *Yearbook of Private International Law*, 13, 483-491.
- Common. In L. Floridi & M. Taddeo (Eds.), *The Responsibilities of Online Service Providers*, Wien, Springer. <http://dx.doi.org/10.2139/ssrn.2839213>
- Gumzej N. (2016). EU pravo na zaborav i globalni internet: izvršavanje zahtjeva za uklanjanje poveznica na pretraživačima [EU right to be forgotten and global internet: enforcement of delinking requests]. *Media, culture and public relations*, 7(2), 171-191. Retrieved from <https://hrcak.srce.hr/176512>
- Harvey, R. E. (2019). Host providers may be subject to obligations resulting in content removal on a worldwide basis, says AG Szpunar. *Journal of Intellectual Property Law & Practice*, 14(11), 836-838. <https://doi.org/10.1093/jiplp/jpz116>
- Johnson, N. L., Johnson, D. L., Tweed, P. & Smolla, R. A. (2019). *Defamation and invasion of privacy in the internet age*. Southwestern

- Journal of International Law, 25(1), 9-41. Retrieved from <https://www.swlaw.edu>
- Knol Radoja, K. (2015). Pretpostavke dopuštenosti podnošenja tužbe u odnosu na određene pravne subjekte [The prerequisites to bring an action in respect of certain legal entities]. Doctoral thesis, Osijek, Pravni fakultet u Osijeku
- Knol Radoja, K. (2018). Utjecaj odredbi o nadležnosti na razinu zaštite prava na privatnost u Europskoj uniji [The effect of the provisions of the jurisdiction on the level of protection of the right to privacy in the European Union]. International Counseling "Actualities of Civil Procedure Rights - National and Comparative Legal and Practical Achievements", Split, 213-234.
- Koziol, H. (2005). Recht auf korrekte Information durch Massenmedien und privatrechtlicher Schutz?, In: S. Lorenz, A. Trunk, H. Eidenmüller, C. Wendehorst & J. Adolff (Eds.), Festschrift für Andreas Heldrich zum 70. Geburtstag, München, C.H. Beck
- Koziol, H. (2005a). Protection of personality rights against invasions by the mass media: summary and outlook. In: H. Koziol, & A. Warzilek (Eds.), The protection of personality rights against invasions by mass media, Wien, New York, Springer
- Kuczerawy, A. (2019). General monitoring obligations: a new cornerstone of internet regulation in the EU? Rethinking IT and IP Law - Celebrating 30 years CiTiP, Intersentia, 141-148. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3449170
- Munivrana Vajda, M., Šurina Marton, A. (2016). Gdje prestaju granice slobode izražavanja, a počinje govor mržnje? Analiza hrvatskog zakonodavstva i prakse u svjetlu europskih pravnih standarda [Where does the right to freedom of expression end and hate speech begin? An analysis of Croatian legislation and jurisprudence in the light of European legal standards]. Hrvatski ljetopis za kaznene znanosti i praksu, 23(2), 436–438. Retrieved from <https://hrcak.srce.hr/177439>
- Revalidis, I. (2017). Judicial jurisdiction over internet privacy violations and the GDPR: a case of „privacy tourism“. Masaryk University Journal of Law and Technology, 11(1), 7–37. <https://doi.org/10.5817/MUJLT2017-1-2>
- Ružić, N. (2008). Zakonska ograničenja ili sloboda izražavanja na internetu? [Legal restrictions or freedom of expression on the Internet?]. MediAnali: međunarodni znanstveni časopis za pitanja medija, novinarstva, masovnog komuniciranja i odnosa s javnostima, 2(4), 101-111. Retrieved from <https://hrcak.srce.hr/39349>
- Samonte, M. (2017). Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law. European papers, 9(3), 839-851. Retrieved from http://www.europeanpapers.eu/en/system/files/pdf_version/EP_EF_2020_I_003_Mary_Samonte_0.pdf
- Skoko, B., Bajsić, D. (2007). Objavljivanje neistina i manipuliranje činjenicama u hrvatskim medijima i mogućnosti zaštite privatnosti, časti i ugleda

- [Reporting untruths and manipulating facts in croatian media, and possibilities for protecting privacy, honour and reputation]. *Politička misao*, 44(1), 93–116. Retrieved from <https://hrcak.srce.hr/20149>
- Stratford, J. (2002). *Striking the balance: privacy and freedom of expression under the European convention on human rights*. In M. Colvin (Ed.), *Developing Privacy Rights*, Oxford, Hart Publishing
- Svantesson, D. (2019). Grading AG Szpunar's opinion in case c-18/18 a caution against worldwide content blocking as default. *Masaryk University Journal of Law and Technology*, 13(2), 389-400, <https://doi.org/10.5817/MUJLT2019-2-10>
- Tagaras, H. (2015). *Comparative Law and the European Union Civil Service Tribunal*. In M., Andenas & D., Fairgrieve (Eds.), *Courts and Comparative Law*, Oxford, OUP Oxford
- Valcke, P., Kuczerawy, A., Ombelet, P. J. (2016). Did the Romans get it right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in
- Vasquez, M. L. (2020). Culture, religion, and the new geographies of law troubling takedowns in 'Ewa Glawischnig-Piesczek v. Facebook Ireland Ltd'. *CALUMET – intercultural law and humanities review*, 57-79. Retrieved https://www.academia.edu/42027202/Culture_Religion_and_the_New_Geographies_of_Law_Troubling_Takedowns_in_Ewa_Glawischnig-Piesczek_v._Facebook_Ireland_Ltd
- Vodinelić, V. (2003). *Pravo masmedija [The right of the mass media]*. Beograd, Fakultet za poslovno pravo u Beogradu

Regulations, acts and court decisions

- C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgment of 13 May 2014.
- C-507/17, *Google Inc v Commission nationale de l'informatique et des libertés (CNIL)*, judgment of 24 September 2019.
- Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, judgment of 3 October 2019.
- Charter of Fundamental Rights of the European Union, 2012/C 326/02, OJ C 326, 26.10. 2012, 391.–407.
- Convention for the Protection of Human Rights and Fundamental Freedoms, Official Gazette, International Treaties, no. 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10.
- 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, OJ L 178, 17.7.2000.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

processing of personal data and on the free movement of such data, OJ L 281/31.

Opinion of Advocate General Szpunar in *Glawischnig-Piesczek* (C-18/18, EU:C:2019:458)

Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 012, 16/01/2001 P. 0001 - 0023.

Regulation (EU) (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 351, 20.12.2012, p. 1–32.

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, OJ L 119, 4.5.2016, p. 1–88.

Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark, OJ L 154, 16.6.2017, p. 1–99.

Universal Declaration of Human Rights, Official Gazette, International Treaties, no. 12/2009.

Website references

Fleischer, P. (2015). Implementing a European, not global, right to be forgotten. Retrieved 23 March 2020 from <http://googlepolicyeurope.blogspot.de/2015/07/implementing-european-not-global-right.html>

Rufer, A. (2015). The creeping "right to be forgotten", *The News Media and The Law*, 2015, 39(1). Retrieved 24 March 2020 from https://www.rcfp.org/wp-content/uploads/2019/01/Winter_2015.pdf

Sartor, G. (2017). 'Providers Liability: From the eCommerce Directive to the future' European Parliament, Directorate General for Internal Policies Policy Department A: Economic and Scientific Policy (October 2017). Retrieved 11 March 2020 from [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA\(2017\)614179_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf)

Woods, L. (2019). Facebook's liability for defamatory posts: the CJEU interprets the e-commerce Directive. Retrieved 19 March 2020 from <http://eulawanalysis.blogspot.com/2019/10/facebooks-liability-for-defamatory.html>

