Towards a wider scope for the duty of care of host internet service providers: The case of *Eva Glawischnig-Piesczek v Facebook*

I. Legal Context

In the *Eva Glawischnig-Piesczek v Facebook* [1] the CJEU takes the opportunity to take a step forward with regard to the concept of duty of care of host internet service providers.[2] It deviates from the existing judicial approach and deploys a wider interpretation of the scope of a duty of care; imposing a set of broader obligations to host ISPs. By duty of care shall be understood a set of obligations that are ascribed to host ISPs with the aim to terminate the dissemination of infringing content within their networks. The legal framework within which this case has been examined is to be found in the e-Commerce Directive.[3] In particular, Article 14 (1) of the e-Commerce Directive addresses the liability of host ISPs and sets out the circumstances under which host ISPs cannot be liable for the infringements that are committed by their users. Namely, host ISPs can escape liability if they lack knowledge of the infringing content or if they expeditiously remove the infringing content upon being notified.

Another provision which is relevant to this case is Article 15 (1) of the e-Commerce Directive that prohibits the imposition of general monitoring obligations to host ISPs. This means that host ISPs are not obliged to deploy filtering-based technology in order to control the dissemination of content and information within their networks. However, a duty of care in specific cases is not precluded. As per Recital 47 of the e-Commerce Directive, Member states are allowed to impose monitoring obligations to host ISPs in specific cases, while Recital 48 of the e-Commerce Directive requires host ISPs to adopt preventive measures in order to identify and prevent certain kinds of wrongdoings.

[1] Case C-18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821.
[2] Hereinafter host ISPs.
[3] Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular, electronic commerce, in the Internal Market (2000) O.J. L 178.

The case of *Eva Glawischnig-Piesczek v Facebook* is added to a bedrock of rulings where the courts have issued injunctive relief against host ISPs in cases of online infringements, such as defamation, copyright or trade mark violations, committed by their internet users. Such cases have been examined at national and European level and set out the requirements for imposing a duty of care to host ISPs with regard to the dissemination of unlawful information online.

II. Facts

In the case at hand, an internet user posted on Facebook an article from an online journal about Eva Glawischnig-Piesczek, a former Austrian politician and member of the Green Party, accompanied with a number of defamatory comments about her. On the 7th of July 2016, the claimant, Eva Glawischnig-Piesczek, sent a notification to Facebook and asked for the removal of the unlawful post. Having received no response, the claimant pursued legal proceedings at the Commercial Court of Vienna requesting Facebook to delete the defamatory posts as well as to prevent the uploading of any identical or equivalent comment to the defamatory post. On appeal, the Higher Regional Court of Vienna confirmed the order of the Commercial Court only with regard to the removal of identical comments to the defamatory post. The case then has been appealed to the Austrian Supreme Court that decided to stay at the proceedings and made a preliminary reference to the Court of Justice of the European Union,[4] requesting clarification as to whether Article 15 (1) of the e-Commerce Directive excludes host ISPs from the obligation to remove identically illegal content, or content equivalent to the already illegal content, and whether this obligation could be applied worldwide.

III. Analysis

On the 3rd of October 2019, the CJEU delivered its long-awaited judgement and concluded that Article 15 (1) of the e-Commerce Directive does not preclude host ISPs from removing identical content of information that has already been declared unlawful, and equivalent information, without requiring the host ISPs to conduct independent examination of that content. It added that such an obligation shall have a worldwide application.

[4] Hereinafter CJEU.

However, whereas the Court's conclusion echoes the Advocate General's opinion as to the imposition of a duty of care on host ISPs, it articulates a wider scope for duty of care. Interestingly, it is this wider scope for a duty of care which might raise concerns with regard to its compatibility with the *EU acquis*. In this light, this article aims to highlight the problematic aspects of this decision and, in particular, those aspects that might threaten the business welfare of host ISPs, the fundamental rights of users and the personality rights of victims of defamatory comments.

A. A duty of care on host ISPs: legislative, policy and judicial trends

At the outset, the imposition of obligations to host ISPs is explicitly included at legislative level. Indeed, a duty of care in specific cases is envisaged in Recital 47 of the e-Commerce Directive which states that host ISPs can deploy preventive measures against online infringements only in specific cases.

At policy level, the ascription of a duty of care of host ISPs has been reiterated in a plethora of policy initiatives at national and international level. For instance, under the umbrella of unlawful speech, the code of conduct on illegal hate speech encourages ISPs to adopt proactive measures and remove any content related to unlawful speech.[5] In this vein, Facebook offers a defamation reporting form[6] while Dailymotion[7] and Vimeo[8] notify their users that any content related to defamatory or hate speech will be removed. The success of this policy initiative has been demonstrated by the Progress Report which states that 72% of illegal content is taken down, while ISPs manage to examine 89% of the illegal content within 24 hours.[9] Likewise, the European Commission's Communication on Disinformation in 2018 provides a set of recommendations to ISPs, such as the use of artificial intelligence technology in order to locate and flag disinformation.[10] Further, UNESCO's Handbook on hate speech and disinformation criticizes the role of ISPs as online gatekeepers and pushes for greater responsibility insofar as the dissemination of fakes news is concerned.[11] Likewise, at the European level the Proposal for a Digital Services Act ascribes a set of obligations to very large online intermediaries. Such

[5] Code of conduct countering illegal hate speech online, Facebook, Microsoft, Twitter and YouTube.
[6] https://www.facebook.com/communitystandards/bullying
[7] https://faq.dailymotion.com/hc/en-us/articles/203839126-Content-policies-and-inappropriate-content
[8] https://vimeo.com/help/guidelines
[9] EU Commission Progress report, "Code of conduct countering illegal hate speech" (February 2019) 1
[10] EU Commission, "Communication on tackling online disinformation: a European approach" (2018) COM 236 final 11.
[11] Unesco, *Journalism, Fake News and Disinformation* (2018) 64-65.

obligations vary from the adoption of content moderation technologies to the issue of transparency reports on a mandatory basis.[12] Moreover, at national level, the UK White paper on online harms[13] announces a statutory duty of care for host ISPs in order to guarantee online safety and limit incidents of abuse, harassment and hate speech against online users. Finally, at legislative level, Germany and recently France have introduced a duty of care for host ISPs with regard to the dissemination of hate speech online. Pursuant to the German Enforcement Networks Law (Netzwerkungsgesetz), ISPs must remove any unlawful speech related content within 24 hours.[14] Lack of compliance might result to fines of up to 50 million euros. Insofar as French law is concerned, the French Parliament voted on the 13th of May 2020 the Avia Law (Loi Avia) that requires host ISPs to remove within 24 hours offensive content such as hate speech comments. Lack of compliance might trigger fines of up to 4% of their annual global turnover.[15]

However, the ascription of a duty of care on host ISPs is not limited to policy and legislative level. Indeed, at judicial level the trend of duty of care finds its roots back to *L'Oreal v eBay*.[16] In this case, L' Oreal brought legal proceedings against eBay alleging trade mark infringement because eBay displayed counterfeit L'Oreal goods within its network. After a careful consideration of the facts, the CJEU concluded that eBay shall not only terminate the trade mark infringements but also prevent the same trade mark infringements offered by the same seller. This implies that eBay shall deploy preventive measures with the aim to curb the circulation of counterfeit L'Oreal goods.

Within the context of defamation, duty of care has been confirmed for the first time in the *Delfi* case.[17] In this dispute, the Supreme Court of Estonia found Delfi, a popular news portal , liable for not preventing the repost of defamatory comments against an internet user. Delfi initiated legal proceedings against Estonia alleging interference with their right to freedom of expression, as per Article 10 of the European Convention of Human Rights. In 2015, the Grand Chamber of the

[12] Article 25 and Recital 58 of the "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" COM (2020) 825 final.
[13] UK White Paper on online harms (April 2019) is available at < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf > last accessed 10 February 2021.
[14] ARTICLE 19, "Germany: The Act to Improve Enforcement of the Law in Social Networks" (2017) is available at < https://www.article19.org/wp-content/uploads/2017/09/170901-LegalAnalysis-German-NetzDG-Act.pdf > last accessed 10 February 2021.
[15] Loi n° 2020-766 du 24 juin 2020, Loi Avia is available at < https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970 > last accessed 10 February 2021.
[16] Case C-324/09, *L'Oreal SA V eBay Int'l AG* (2011) ECR. I-6011.
[17] ECtHR, Grand Chamber, *Delfi AS v Estonia* (16 June 2015) Application no. 64569.

European Court of Human Rights examined the compatibility of the duty of care on host ISPs with Article 10 of the European Convention of Human Rights and concluded that any interference with the right to free expression shall be prescribed by law, pursue the legitimate aims of para. 2 of Article 10 and be necessary in a democratic society.[18] In that case, Delfi was a professional publisher that was operating a popular news portal and thus could have foreseen the risks and the implications of its services as set forth in civil law provisions.[19] In addition, the Grand Chamber found that the restriction of free speech was justified and proportionate[20] and had the legitimate aim of protecting the reputation and rights of others.[21] Therefore, it appears that a duty of care to host ISPs could be applied under specific conditions.

B. *Eva Glawischnig-Piesczek v Facebook*: a wider scope of a duty of care and its compatibility with the EU acquis

The *Eva Glawischnig-Piesczek v Facebook* case confirms the imposition of a duty of care on host ISPs but offers a wider interpretation thereof. In particular, this wider scope of a duty of care entails a set of broader obligations for host ISPs, such as the use of content identification technology, in order to remove the equivalent to the declared defamatory content and the removal of the defamatory post on a worldwide basis. Yet, such obligations, as thoroughly discussed below, are not compatible with a cluster of EU provisions.

i. The concept of equivalent information

Reinforcing the wording of the referring national court,[22] the CJEU concluded that the host ISP must terminate or prevent the reemergence of identical and equivalent content. Identical content addresses the same "content of information which was previously declared to be illegal"[23] and equivalent information is about the "information conveying a message the content of which remains essentially unchanged and therefore diverges very little from the content which gave rise

[18] Although the dissenting views have criticized the application of preventive measures in the form of a duty of care.
[19] ECtHR, Grand Chamber, *Delfi AS v Estonia* (16 June 2015) Application no. 64569, para. 62.
[20] ECtHR, Grand Chamber, *Delfi AS v Estonia* (16 June 2015) Application no. 64569, para. 65.
[21] *Delfi AS v Estonia* (16 June 2015) Application no. 6456, para. 63.
[22] Case C-18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para. 20.
[23] Case C-18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para. 37.

to the finding of illegality."[24] While the term 'identical information' is easily understood, the concept of 'equivalent information' seems unclear. For instance, one might wonder what is meant by essentially unchanged content or content which differs very little from that which has been declared unlawful.

In order to clarify this uncertainty, the CJEU stated that the equivalent information to unlawful content does not rest upon the syntactical or orthographical use of certain terms. Rather, it emerges from the illegal nature of the content transmitted.[25] In the case of Facebook, it concerns the illegal nature of the content which was defamatory to the individual.

This understanding, however, might prompt reflections on the role of host ISPs as adjudicators of content.[26] This is because one might wonder whether a host ISP has the ability to determine the legality of the content, or otherwise, within the concept of equivalent information. Defamatory infringements are contextual infringements.[27] This means that in order to determine whether a comment is defamatory, there must be knowledge of the context within which the illegal message is disseminated online. As Franklin and Bussel point out "Context can convert a seemingly innocuous statement into a defamatory one and vice versa."[28] On the one hand, consider, for instance, cases where a defamatory comment is reposted by a user who criticizes the content thereof, or where a defamatory comment is reposted by a user in the context of news communication. Lack of knowledge of the context might lead to the removal of lawful content and thus restrict users' right to impart and receive information as set forth in Article 11 of the EU Charter of Fundamental Rights.[29]

[24] Case C-18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para. 39.
[25] Case C-18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para. 40.
[26] A similar discussion was raised in M. Perel and N. Elkin-Koren, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 Stanford Technology Law Review 485.
[27] Similar to copyright infringements, see also M. Husovec, "Accountable, Not Liable: Injunctions Against Intermediaries" (2016) TILEC Discussion Paper 37.
[28] M. Franklin and D. Bussel, "The Plaintiff The Plaintiff's Burden in Defamation: A den in Defamation: Awareness and Falsity" (1984) 25 William & Mary Law Review 830.
[29] Opinion of the Advocate General Szpunar in Case C- 18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:458, para. 74 where he pointed out that "freedom of expression and information might well be systematically restricted".

On the other hand, consider the case where the offender uses totally different words and thus continues the defamation of a specific individual, or the case where the offender continues the defamation by using irony. The latter example can be seen in the case of Lord McAlpine, against whom a number of defamatory tweets were posted. In this case, the offender tweeted the following comment, "why is Lord McAlpine trending? innocent face."[30] Yet, although the offender argued that it was simply a question, the English court concluded that "the reasonable reader would understand the words "innocent face" as being insincere and ironical."[31] Therefore, lack of knowledge of the context might enable the offender to continue the defamation.

What is more, the knowledge of the context could be obtained through filtering-based tools. Yet, such filtering technology has been subject to severe criticism among scholars. This is because filtering based technology could perform marginal errors and remove lawful content.[32] Indeed, a study conducted by Jacques, Garstka, Hviid and Street points out that while in January 2012, 1845 parody videos from music songs were available on YouTube, in December 2016 32.1% of them were removed from Content ID system under the justification of copyright infringement.[33] In addition, a number of documented wrongful removals illustrate the flaws of content identification systems. An example of this is the removal of a political video on YouTube. This video concerned the speech of a Member of the EU Parliament who advocated the termination of selling trade goods that are used for torture and death penalties.[34] The video was removed under the justification of violating the community guidelines of the online music-exchange platform. However, the removal of this video has deprived EU citizens from obtaining knowledge of a highly important discussion topic.[35] Likewise, another example can be found in a video from the Black Lives Matter protests.[36] This video was removed from YouTube and Facebook for copyright infringement because snippets of popular songs were played during the protests by the

[30] *McAlpine v Bercow* (2013) EWHC 1342 (QB), para. 3.
[31] *McAlpine v Bercow* (2013) EWHC 1342 (QB), para. 84.
[32] BILETA, 'Written Evidence for the House of Lords, Select Committee on Communications; The Internet: To regulate or not to regulate: Summary or response' 3; A. Bridy and D. Keller, "U.S. Copyright Office Section 512 Study: Comments in Response to Notice of Inquiry" (31 March 2016) 20.
[33] S. Jacques, K. Garstka, M. Hviid and J. Street, "The Impact on Cultural Diversity of Automated Anti-Piracy Systems as Copyright Enforcement Mechanisms: An Empirical Study of YouTube's Content ID Digital Fingerprinting Technology" (2018) 15 SCRIPTed 298.
[34] J. Reda, "When filters fail: These cases show we can't trust algorithms to clean up the internet" (Reda's website, 28 September 2017) is available at < https://juliareda.eu/2017/09/when-filters-fail/ > last accessed 18 May 2019.
[35] Ibid.
[36] M. Masnick, "Copyright Blocks Interview Of Protesters Because Marvin Gaye's 'Let's Get It On' Was Playing In The Background" (Techdirt, 3 June 2020) is available at < https://www.techdirt.com/articles/20200602/21391944634/copyright-blocks-interview-protesters-because-marvin-gayes-lets-get-it-was-playing-background.shtml > last accessed 10 February 2021

participants. Therefore, it appears that the adoption of filtering mechanisms might give rise to censorship and thus encroach upon the right to freedom of expression of internet users.[37]

Further, the CJEU included into the scope of the duty of care of host ISPs any uploaders of equivalent information to defamatory contents. Differentiating its ruling from the Opinion of the Advocate General, who limited the duty of care of host ISPs to the initial offender who posted the defamatory comment,[38] the CJEU did not restrict the removal of posts to the initial uploaders of defamatory comment. Rather, under the reasoning of ease spread of content due to digitalization, it was argued that "there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network."[39] This implies that host ISPs have an obligation to take down posts from any user who uploads unlawful information.

Moreover, this outcome does not only differ from the AG's opinion. Rather, it deviates from previous rulings at European level too. This is because it differentiates from the *L'Oreal v eBay* case, which provided a narrow interpretation of duty of care. As already flagged, in the *L' Oreal v eBay* case, the scope of a duty of care was limited trade mark infringements of the same nature committed by the same trader.[40] In a similar fashion, the *Eva Glawischnig-Piesczek* case differentiates from the *Delfi* case where the Grand Chamber of the Court of Human Rights confirmed the compatibility of a duty of care on host ISPs with Article 10 of the European Convention of Human Rights.[41] As per the Court's decision, the ascription of a duty of care on host ISPs shall be prescribed by law, complete one of the aims of the Article 10 of the European Convention of Human Rights and be necessity for a democratic society. Otherwise, a duty of care would intervene with the data subject's fundamental rights and would be deemed unlawful.

ii. The use of automated search tools and technologies

[37] Center for Democracy and Technology, "Mixed Messages? The Limits of Automated Social Media Content Analysis" (November 2017) 11 where it is stated that "an accuracy rate of 80% means that one out of every five people is treated "wrong" in such decision-making; depending on the process, this would have obvious consequences for civil liberties and human rights."
[38] Opinion of the Advocate General Szpunar in Case C 18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:458, para. 55.
[39] Case C 18/18, *Eva Glawischnig-Piesczek* (2019) ECLI:EU:C:2019:821, para. 36.
[40] Case C-324/09, *L'Oreal SA V eBay Int'l AG* (2011) ECLI:EU:C:2011:474, para. 141.
[41] ECtHR, Grand Chamber, *Delfi AS v Estonia* (16 June 2015) Application no. 64569.

The CJEU held in para. 31 that, while the imposition of general monitoring obligations is prohibited under Article 15 (1) of the e-Commerce Directive, monitoring is allowed under specific cases as per this directive's Recital 47.[42]

However, the statement of the CJEU lacks essence. This is because, in para. 46, the use of automated technological tools is explicitly introduced. To the Court's reasoning "defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies."[43] This means that, in order to determine the equivalent information to defamatory comment, the use of content identification systems is allowed.

a. Crossing the lines with Article 15 of the e-Commerce Directive

Importantly, this understanding might come under fire since the use of automated content identification might come in conflict with Article 15 of the e-Commerce Directive.[44] Article 15 of the e-Commerce Directive was introduced in 2000 when the e-commerce was at its infancy[45] and its main aim was to boost innovation and not to burden host ISPs. The use of filtering-based technology might place an onus on host ISPs who might lack of resources to license or develop that kind of technology. In this light, new host ISPs might be hesitant to enter the Digital Single Market, while other host ISPs might be forced to shut down their businesses and, thus, their fundamental right to conduct business as per Article 16 of the EU Charter of Fundamental Rights would be violated.

What is more, one might wonder how it is possible to deploy automated content technology and not ascribe general monitoring to host ISPs. As Advocate General Villalon in *Scarlet v Sabam*[46] has

[42] For debate between Article 15 of the ECD and Recital 47 of the ECD see J.P. Quintais, "The New Copyright in the Digital Single Market Directive: A Critical Look" (2019) 1 European Intellectual Property Review 28-41.
[43] Case C 18/18, *Eva Glawischnig-Piesczek* (2019) ECLI:EU:C:2019:821, para. 46.
[44] At legislative level, the concept of content identification systems is already introduced at policy level. For instance, see the EC, "Assessment of the Code of Conduct on Hate Speech on line State of Play" (2019) 12522/19; Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM/2016/0593 final; Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (2018) OJ L 95, 15.4.2010; Proposal for a Regulation on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 COM/2018/640 final.
[45] D. Friedmann, "Sinking the safe harbour with the legal certainty of strict liability in sight" (2014) 9 JIPLP 148.
[46] Opinion of the Advocate General Villalon in Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECLI:EU:C:2011:255.

rightfully pointed out, "The object of the monitoring is specifically defined as having to make it possible to filter the electronic communications passing through Scarlet's services, both incoming and outgoing"[47] while he also noted with regard to filtering, "To be effective, it must be at the same time systematic, universal and progressive."[48] This understanding has been reinforced by an array of filtering-based technological tools which offer general network monitoring and filter all communications online, for instance, hash-based identification technology.[49] An example can be found in the PhotoDNA software developed by Microsoft which identifies terroristic and child abuse content.[50] Such technology uses hashes which constitute a unique digital signature for each file and compare one file against other files in a database.[51] Should the hash of a file match with the hash of one of the other files, then a terroristic or a child abuse material is located. Another kind of technology is fingerprinting-based software, of which examples can be found in Content ID system or Cleanfeed software or Audible Magic software. Content ID system, developed by YouTube, aims at blocking copyright infringing videos that users have uploaded on YouTube. The official website of YouTube defines how Content ID operates and notes that "…Videos uploaded to YouTube are scanned against a database of files that have been submitted to us by content owners."[52] Cleanfeed technology ,which was suggested by Arnold Justice in the *Twentieth Century* case, aims at blocking child-abuse content by "examining all traffic flowing from customers."[53] Audible Magic software was discussed in the *Scarlet v Sabam* case and aims at automatically inspecting internet communications.[54] For this reason, Angelopoulos aptly remarked "….only with

[47] Opinion of the Advocate General Villalon in Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECLI:EU:C:2011:255, para. 48.
[48] Ibid.
[49] G. Sartor and A. Loreggia, Study requested by the JURI committee on "The impact of algorithms for online content filtering or moderation: upload filters" (2020) 40.
[50] G. Frosio and M. Husovec, "Accountability and Responsibility of Online Intermediaries" in G. Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 613-640.
[51] "How does PhotoDNA technology work?" is available at <https://www.microsoft.com/en-us/photodna> last accessed 18 May 2020.
[52] "How Content ID works" is available at <https://support.google.com/youtube/answer/2797370?hl=en-GB> last accessed 10 February 2021
[53] *Twentieth Century Fox v. Newzbin Ltd* [2010] EWHC 608 (Ch) para. 31; Arnold Justice recommended the adoption of Cleanfeed, which is a filtering technology, and which has proved to be technically feasible and not easily circumvented by users; R. Clayton, "Failures in a Hybrid Content Blocking System" (2018) 2 is available at <https://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf > where Clayton notes that "The CleanFeed system is a hybrid design, incorporating both redirection of traffic and the use of web proxies. It is intended to be extremely precise in what it blocks, but at the same time to be low cost to build and operate."
[54] Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011) ECLI:EU:C:2011:771, para. 47.

difficulty can the digital fingerprinting technology employed by Audible Magic be considered distinct from general monitoring activities."[55]

However, the use of automated content identification tools do not only come in conflict with Article 15 (1) of the e-Commerce Directive. Indeed, it also seems difficult to reconcile with a bedrock of case law at the European level. Consider, for instance, the case of *Scarlet v Sabam*.[56] In this case, Sabam, which is the Belgian association for authors, requested a filtering injunction against Scarlet, an internet access service provider, alleging copyright infringement. Sabam argued that Scarlet's subscribers use its network in order to file-share unauthorized material peer to peer. However, the Court refused to issue an injunction under the reasoning that the imposition of a filtering obligation would "oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual property rights…"[57]

Such a stance was maintained in *Sabam v Netlog*[58] where the CJEU rejected for a second time the application to order a filtering injunction. In this case, Sabam requested a filtering injunction against Netlog, a social network platform, alleging copyright infringements. Sabam argued that Netlog's users uploaded unauthorized material on the platform, such as films and songs from its film repository. Yet, drawing parallels with the *Scarlet v Sabam* ruling, the CJEU refrained from issuing a filtering injunction under the reasoning that the injunction would require to "actively monitor almost all the data relating to all of its service users.."[59]

Along similar lines, in the *McFadden*[60] ruling, a dispute between the owner of a wifi connection that does not require a password to access internet and Sony Music, the CJEU delivered that the use of filtering-based technology would monitor all the information that is transmitted and

[55] C. Angelopoulos, "Filtering for Copyrighted Content in Europe" (2009) IRIS plus 5; see also Audible Magic Presentation to DG Connect (2017) 50- 51 is available at <https://www.asktheeu.org/en/request/4465/response/14429/attach/5/Annex%20I%20Gestdem%202017%204050%20v3.pdf > where it is stated that the software operates 24 hours per day, each day of the week and most importantly it does not require the involvement of the internet service provider or the right holder.

[56] Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011) ECLI:EU:C:2011:771.

[57] Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011) ECLI:EU:C:2011:771, para. 40.

[58] Case C-360/10, *Belgische Vereniging van Auteurs, Com- ponisten en Uitgevers CVBA (SABAM)* v. *Netlog NV* (2012) ECLI:EU:C:2012:85.

[59] Case C-360/10, *Belgische Vereniging van Auteurs, Com- ponisten en Uitgevers CVBA (SABAM)* v. *Netlog NV* (2012) ECLI:EU:C:2012:85, para.37.

[60] Case C-484/14 - *McFadden* (2016) ECLI:EU:C: 2016:689.

therefore it contradicts with Article 15 (1) of the e-Commerce Directive which prohibits general monitoring obligations.[61]

Therefore, it appears that the use of content identification tools is not compatible with the prohibition of general monitoring obligations as this has been set forth in Article 15(1) of the e-Commerce Directive and in a line of case law at European level.

b. In conflict with Article 22 of the General Data Protection Regulation

Further, the use of automated search tools and technologies, as held by the Court in para. 46, might prompt reflections with regard to its compatibility with the General Data Protection Regulation provisions and, in particular, with Article 22 which states that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." This means that the user can object the process of her data if such process has binding legal effects for her.

This is because profiling is part of the automated process of data which constitutes the main function of content identification technologies.[62] As per Article 4, profiling concerns "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person…"

However, it is only under circumscribed conditions where the automated process of data could be lawful. Such conditions may be the performance of a contract, the authorization from a member state or the explicit consent from the data subject.[63] Within the context of defamatory comments, the latter condition could be relevant. In particular, profiling could be lawful when the internet user agrees on the automated process of her data in the terms and conditions. For instance, profiling could be listed under the terms and conditions of host ISPs and the internet user would agree to it by registering.[64] This means that consent shall be explicitly given by the

[61] Case C-484/14 - *McFadden* (2016) ECLI:EU:C: 2016:689, para. 87.
[62] ICO, "What is automated individual decision-making and profiling?" is available at < https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/ > last accessed 19 May 2020.
[63] Article 29 Data Protection Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (2018) 25.
[64] G. Frosio, "Algorithmic enforcement online" in P. Torremans (ed.), *Intellectual Property and Human Rights* (4th edition, Kluwer Law International 2020) 17-18.

data subject. Such consent shall be freely given, specific, and informed either as an express statement or an affirmative action.[65] Yet, such consent requires that the data subject shall be clearly informed about the rationale and the purposes of the profiling. This understanding has been outlined by the Council of Europe whose recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling outlined that "The data subject who is being, or has been, profiled should be entitled to obtain from the controller, at her or his request, within a reasonable time and in an understandable form, information concerning: a. her or his personal data; b. the logic underpinning the processing of her or his personal data and that was used to attribute a profile to her or him, at least in the case of an automated decision; c. the purposes for which the profiling was carried out and the categories of persons to whom or bodies to which the personal data may be communicated."[66] Consider, for instance, the case of Facebook. In the terms and conditions, Facebook shall have a separate section where it explains to its users the use of content identification technology in order to identify defamatory comments, and explain the rationale and the purposes of that automatic process of data.[67] Otherwise, data processing would be deemed unlawful under the General Data Protection Regulation provisions.

c. In conflict with Article 47 of the EU Charter of Fundamental Rights

Finally, the use of automated search tools and technology might encroach upon the right to an effective remedy and a fair trial as set forth in Article 47 of the EU Charter of Fundamental Rights. This provision, as Piątek notes, "treats about a fair and public hearing. During the procedure both sides of the dispute should have a possibility to present and defend their statements."[68] This means that each party in a dispute shall be granted the same rights and not be placed in a less

[65] Article 29 Working Party, "Guidelines on consent under Regulation 2016/679" (2018) 5; Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (2018) 709-744

[66] Council of Europe, "The protection of individuals with regard to automatic processing of personal data in the context of profiling" Recommendation CM/Rec (2010)13 and explanatory memorandum 13.

[67] https://www.facebook.com/legal/terms/dataprocessing

[68] W. Piątek, "The right to an effective remedy in European law: significance, content and interaction" (2019) 6 China- EU Law Journal 167; W. Rubenstein, "The concept of equality of in civil procedure" (2002) 23 Cardozo Law Review 1867-1868 where he explains that "Our adversary system is premised upon the idea that the most accurate and acceptable outcomes are produced by a real battle between equally-armed contestants; thus the adversary system requires, if it is to achieve these goals, some measure of equality in the litigants' capacities to produce their proofs and arguments."

favourable position against the other party.[69] In the case of host ISPs, this means that once users are informed that their material has been removed, they can then seek a recourse of their rights.

Yet, the use of automated search tools does not comply with the right to a fair trial. This is because users are not offered on a mandatory basis the option to submit counter-notifications. Any counter-notification service is left to the discretion of host ISPs and therefore it is up to them to decide whether or not they would notify the allegedly offender once her post has been removed, or give her the opportunity to apply for reinstatement of her post. Hence, without an effective review system, procedural users' rights would be jeopardised and, since the material would remain hidden, users' rights to impart information and prevent other users from accessing it would be impeded.[70]

iii. Removal of unlawful content on an extra-territorial basis and its implications for defamation disputes

Another problematic aspect of this case is the removal of unlawful content worldwide. As the Court stated in para. 53, Article 15 (1) of the e-Commerce Directive does not preclude from "ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law."[71] This means that host ISPs could take down any defamatory post on a global basis.

However, the CJEU refrained from clarifying how this removal would take place worldwide. Instead, it passed the hot potato to the EU member states. To the Court's reasoning "It is up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules."[72] Yet, this understanding might lead to conflicting outcomes with regard to the success of defamatory cases.

[69] ECtHR, "Guide on Article 6 of the European Convention on Human Rights" (2020) 33
[70] S. Kaleda, "The role of the principle of effective judicial protection in relation to website blocking injunctions" (2017) 8 Journal of Intellectual Property, Information Technology and e-Commerce Law 222-223.
[71] Case C 18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para. 53.
[72] Case C 18/18, *Eva Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para. 52.

This is because the substantive laws of defamation are not subject to harmonisation.[73] For instance, what is understood as unlawful comment in one jurisdiction may not be unlawful in another jurisdiction. A representative example can be found in the case of publication on matter of public interest or in the case of an honest opinion. While the publication of a statement on matter of public interest or an honest opinion would be unlawful in France, they are valid defences under the UK Defamation Act 2013.[74] This means that the host ISP might remove comments which are considered lawful in one member state and thus encroach upon the right of freedom of expression. Further, the thresholds of defamatory speech might differ from one jurisdiction to another. For example, in some jurisdictions, in order to adjudicate damages for a defamatory post, a certain number of people that have accessed the unlawful content are required. This was the case of *Jameel v Dow Jones*[75] in England. In this case, the Wall Street Journal published a defamatory comment about Mr. Jameel, a businessman from Saudi Arabia. However the English Court dismissed the case due to the fact that only five users had accessed the defamatory post and three of them were already involved in the case. Therefore, the English Court denied to adjudicate the case due to the minimal vindication and damage. As Lord Philipps pointed out "…The game will not merely not have been worth the candle, it will not have been worth the wick."[76]

What is more, in light of this lack of harmonization of defamation laws, some jurisdictions might be more appealing to the victims of offensive comments. Jurisdictions with lower standards of defamation laws might offer legal redress to victims, while others would not. An illustrative example can be found in England. English jurisdiction is considered "the libel capital of the world"[77] because it entails a low threshold for harmful content in comparison to other jurisdictions. This understanding was illustrated in the *Four Seasons Holdings Incorporated v Brownlie*[78] case, where the UK Supreme Court adopted a wider interpretation of the concept of damages by including indirect or consequential financial losses as requirements. Therefore, as

[73] European Commission, "Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality" (2007) JLS/2007/C4/028 Final Report 42-49.
[74] D. Mondoloni, "Legal divisions: French versus English libel laws" (2014) 2 Sage Journals 84.
[75] *Jameel v Dow Jones Inc.* (2005) EWCA Civ. 75.
[76] *Jameel v Dow Jones Inc.* (2005) EWCA Civ. 75, para. 69.
[77] S. James, "Tightening the net: defamation report and ISPs" (2012) Entertainment Law Review 1.
[78] *Four Seasons Holdings Incorporated v Brownlie* (2017) UKSC 80, para. 55.

long as the claimant can prove indirect or consequential harm in the UK, a defamatory claim can be brought in front of the UK courts.

Should the victim wish to seek compensatory or injunctive relief against defamatory comments, the rule of *lex loci delicti* applies.[79] This means that the victim can seek for redress in jurisdiction where the victim suffered harm. This principle stems from Regulation No 1215/2012, otherwise known as the Brussels I Regulation Recast,[80] which addresses the adjudication of defamatory disputes. Yet, in online disputes that harm might occur anywhere in the world. This implies that a victim can bring legal proceedings in whichever country the online content can be accessed. This possibility might bring more applicants in a jurisdiction that seems favourable to the victims. Having to choose amongst different jurisdictions, it seems reasonable for the victim to select a jurisdiction that is favourable to its interests. Hence, forum shopping might be developed.[81]

Such forum shopping, however, might lead to abuse of the fundamental rights of internet users. For example, a study conducted by the Council of Europe outlines that the creation of a favourable jurisdiction might have a detrimental effect on freedom of speech.[82] This is because expensive and long-lasting defamation proceedings, along with the high award of damages, might impede journalists or media from expressing their views. This means that the forum shopping trend might create an environment where individuals would be afraid to express their views and therefore lawful content would not be disseminated to a great extent.

Further, the forum shopping jurisdiction might not be a panacea for the victims of defamatory posts. This is because the decisions issued in the favourable jurisdiction might not be enforceable in a jurisdiction where the defendant has the assets to compensate the claimant. For instance, at the European level, Article 34 of the Council Regulation on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters states that foreign decisions are not

[79] A. Murray, *Information Technology Law* (Oxford University Press 2019) 169.
[80] Council Regulation (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 (2012) OJ L 351.
[81] See also C. Hopkins, "Territorial scope in recent CJEU cases: Google v CNIL / Glawischnig-Piesczek v Facebook" (Inforrm's Blog) is available at < https://inforrm.org/2019/11/09/territorial-scope-in-recent-cjeu-cases-google-v-cnil-glawischnig-piesczek-v-facebook-cathryn-hopkins/ > last accessed 10 February 2021.
[82] Council of Europe, Study on "Liability and jurisdictional issues in online defamation cases" DGI (2019) 26-28.

enforceable in a member state if they are in conflict with the public policy of the member state[83] or are irreconciled with a decision that has been issued in the member state for the same cause between the same parties.[84] Hence, victims of defamatory comments run the risk of not receiving compensation if the foreign decision obtained in the forum shopping jurisdiction is contrary to the public policy of the member state or conflicts with an earlier decision with the same material facts and the same parties.

IV. The way forward

A wider scope of a duty of care for host ISPs, as introduced in the case of *Eva Glawischnig-Piesczek v Facebook,* would pose serious risks to the fundamental rights of host ISPs and internet users. This is because, however useful a duty of care might be for the victims of defamation, the outcome may have a corrosive effect if its limits are not clearly articulated. The adoption of a wider duty of care for host ISPs might impede innovation and jeopardise one of the aims of the Digital Single Market Strategy, which is to maximize the growth of the Digital Economy[85]. In addition, it could trigger a collateral censorship and deprive internet users of their right to freedom of expression and information as set out in Article 11 of the EU Charter of Fundamental Rights.[86]

What is more, the *Eva Glawischnig-Piesczek v Facebook* case might be the precursor of the imposition of a wider duty of care on host ISPs within the context of online defamation disputes. The first influence of the CJEU's ruling was already reported in Austria on the 30th of March 2020 where the Austrian Supreme Court acknowledged the removal of defamatory content on an extraterritorial basis upon the condition that the applicant explicitly requested the worldwide removal of the unlawful content.[87] In addition, on the 16th of July 2020 the Opinion of the Advocate General on *Peterson/ YouTube* required online intermediaries to prevent the

[83] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matter Official Journal (2000) L 012.
[84] M. Petsche, "What's Wrong with Forum Shopping? An Attempt to Identify and Assess the Real Issues of a Controversial Practice" (2011) 45 The International Lawyer 1016
[85] EU Commission, "A Digital Single Market Strategy for Europe" COM (2015) 192 final 13-14.
[86] F. T. Wu, "Collateral Censorship and the Limits of Intermediary Immunity" (2011) 87 Notre Dame Law Review 295-296 where Wu explains that collateral censorship occurs "when a (private) intermediary suppresses the speech of others in order to avoid liability that otherwise might be imposed on it as a result of that speech."; The concept of collateral censorship has been first developed in Balkin's writings; see J. Balkin, "Old School/ new School speech regulation" (2014) 127 Harvard Law Review 2309.
[87] OGH, 30.03.2020, 4Ob36/20b

reemergence of not only identical copyright infringing content, but also equivalent upon the issue of stay down injunctions.[88]

At the same time, similar approaches in other fields of law might be expected in the near future, but not without difficulties. For instance, in the context of terrorism, after the finalization of the EU Regulation on preventing the dissemination of terrorist content online,[89] a wider duty of care could be applied to the host ISPs. In that sense, host ISPs could be required to remove terroristic content on an extraterritorial basis. Within the copyright context, the application of a wider duty of care to host ISPs might be problematic because at judicial level a worldwide removal of the unauthorized content is impeded by the territorial scope of copyright law. Yet, after the full implementation of Article 17 of the Copyright in the Digital Single Market Directive, online content sharing service providers must terminate and prevent the reemergence of unauthorized content. This might imply the use of filtering based tools.[90] Such tools, as already flagged, do not have the ability to determine the instances of copyright infringement in different jurisdictions and, therefore, worldwide removal might take place. Finally, within the context of misinformation, the EU code on Disinformation[91] already requires ISPs to block access to websites that spread misinformation, or terminate accounts of users who post misleading stories on health issues, such as the recent examples of misleading stories about Covid-19 across the EU borders.[92] A worldwide removal of posts such as these could also be applicable.

[88] Opinion of the Advocate General Saugmandsgaard Øe in joined cases C-682/18 and 683/18, *Peterson v YouTube and Elsevier v Cyando* (2020) ECLI:EU:C:2020:586.

[89] Proposal for a Regulation on preventing the dissemination of terrorist content online A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018 COM/2018/640 final

[90] M. Maschnik, "EU Commissioner Gunther Oettinger Admits: Sites Need Filters To Comply With Article 13" (techdirt, 3 April 2019) is available at < https://www.techdirt.com/articles/20190329/15501341902/eu-commissioner-gunther-oettinger-admits-sites-need-filters-to-comply-with-article-13.shtml > last accessed 22 June 2020; Interestingly, companies that develop content identification technologies already advertise their technical tools in relation to Article 17 of the DSMD, see for instance audible magic's website where it states that "Article 17 impacts most social networks in existence today. The clock is ticking, and companies need to put in place technical measures to comply", is available at <https://www.audiblemagic.com/article-17/> last accessed 22 June 2020.

[91] EU Code of Practice in Disinformation (2018)

[92] Council of the European Union, "Fighting disinformation: EU actions to tackle COVID-19 disinformation" is available at < https://www.consilium.europa.eu/en/policies/coronavirus/fighting-disinformation/> last accessed 16 June 2020