Editorial comments: Protecting the EU’s internal market in times of pandemic and growing trade disputes: Some reflections about the challenges posed by foreign subsidies 1365-1382

Articles
M. Wendel, The two-faced guardian – or how one half of the German Federal Constitutional Court became a European fundamental rights court 1383-1426
S. Hindelang and A. Moberg, The art of casting political dissent in law: The EU’S framework for the screening of foreign direct investment 1427-1460
S. Yakovleva, W. Geursen and A. Arnbak, Kaleidoscopic data-related enforcement in the digital age 1461-1494

Case law
A. Court of Justice
Injunctions to remove illegal online content under the eCommerce Directive: Glawischnig-Piesczek, C. Rauchegger and A. Kuczerawy 1495-1526
The Court of Justice on the Junqueras saga: Interpreting the European parliamentary immunities in light of the democratic principle, C. Fasone and N. Lupo 1527-1554
Mandatory labelling of origin of products from territories occupied by Israel and the weight of public international law: Psagot, G. Harpaz 1585-1608
National law cannot exclude damages claims of public lenders against cartelists, Otis v. Land Oberösterreich (Otis II), G. Bacharis 1609-1628

B. National courts
Light and shadows in the Bundesverfassungsgericht’s decision upholding the European Banking Union, P. Faraguna and D. Messineo 1629-1646

Book reviews 1647-1674
Aims
The Common Market Law Review is designed to function as a medium for the understanding and implementation of European Union Law within the Member States and elsewhere, and for the dissemination of legal thinking on European Union Law matters. It thus aims to meet the needs of both the academic and the practitioner. For practical reasons, English is used as the language of communication.
**Subscription information**

2020 Print Subscription Price Starting at EUR 891/ USD 1260/ GBP 635.

Personal subscription prices at a substantially reduced rate as well as online subscription prices are available upon request. Please contact our sales department for further information at +31 172641562 or at International-sales@wolterskluwer.com.

Payments can be made by bank draft, personal cheque, international money order, or UNESCO coupons.

All requests for further information and specimen copies should be addressed to:

Kluwer Law International
P.O. Box 316
2400 AH Alphen aan den Rijn
The Netherlands
fax: +31 172641515

For Marketing Opportunities please contact International-marketing@wolterskluwer.com

Please visit the Common Market Law Review homepage at http://www.kluwerlawonline.com for up-to-date information, tables of contents and to view a FREE online sample copy.

**Establishment and Aims**

The Common Market Law Review was established in 1963 in cooperation with the British Institute of International and Comparative Law and the Europa Instituut of the University of Leyden. The Common Market Law Review is designed to function as a medium for the understanding and analysis of European Union Law, and for the dissemination of legal thinking on all matters of European Union Law. It aims to meet the needs of both the academic and the practitioner. For practical reasons, English is used as the language of communication.

**Editorial policy**

The editors will consider for publication manuscripts by contributors from any country. Articles will be subjected to a review procedure. The author should ensure that the significance of the contribution will be apparent also to readers outside the specific expertise. Special terms and abbreviations should be clearly defined in the text or notes. Accepted manuscripts will be edited, if necessary, to improve the general effectiveness of communication. If editing should be extensive, with a consequent danger of altering the meaning, the manuscript will be returned to the author for approval before type is set.

**Submission of manuscripts**

Manuscripts should be submitted together with a covering letter to the Managing Editor. They must be accompanied by written assurance that the article has not been published, submitted or accepted elsewhere. The author will be notified of acceptance, rejection or need for revision within three to nine weeks. Digital submissions are welcomed. Articles should preferably be no longer than 28 pages (approx. 9,000 words). Annotations should be no longer than 10 pages (approx. 3,000 words). Details concerning submission and the review process can be found on the journal’s website http://www.kluwerlawonline.com/toc.php?pubcode=COLA
CASE LAW

A. Court of Justice

Injunctions to remove illegal online content under the eCommerce Directive: Glawischnig-Pieszcek

Case C-18/18, Eva Glawischnig-Pieszcek v. Facebook Ireland Limited, Judgment of the Court of Justice (Third Chamber) of 3 October 2019, EU:C:2019:821

1. Introduction

Digital platforms such as Facebook or YouTube are modern day gatekeepers. They are therefore often called upon to take a more responsible approach to online content generated by their users. In the EU, such calls have materialized in new policy approaches to online content. In particular, more responsibility and liability for online content has been inserted into the new Directive on Copyright in the Digital Single Market. The Directive includes a highly controversial provision that obliges platform providers to ensure that copyrighted content is not shared without authorization.1 Likewise, a new regulation that is currently being negotiated is likely to introduce monitoring obligations for terrorist online content.2 Moreover, the President of the European Commission, Ursula von der Leyen, put it on the agenda of her term of office to update the general liability regime for digital platforms. The update will take the form of a new Digital Services Act, to be proposed by the end of 2020.3

Currently, the eCommerce Directive is the central legal framework for digital services in the internal market. More than 20 years after it entered into force, it still leaves room for interpretation as far as liability exemptions and monitoring obligations for digital platforms are concerned. In *Glawischnig-Piesczek*, the ECJ was asked to interpret Article 15(1) of the Directive, which prohibits Member States from imposing a general obligation on digital platforms to monitor the content posted by their users.

Specifically, the ECJ was called to clarify what kinds of injunctions a national court could impose on the provider of a digital platform without violating the general monitoring prohibition of Article 15(1) of the eCommerce Directive. The Austrian Supreme Court had asked the ECJ whether it could order Facebook to remove not only an online comment that was found to be defamatory by a court, but also any other comments on the same platform that were identical or equivalent in meaning to the original comment. The ECJ’s answers demonstrated that the Court takes the protection of individuals from illegal online content seriously, following the example of the Union legislature. The judgment surprised many observers around the world, but not in the German-speaking countries.

2. Factual and legal background

The national proceedings in this case concerned an insulting comment on the social media platform Facebook. Eva Glawischnig-Piesczek is the former leader of the Austrian political party The Greens. She was insulted on Facebook by another user. The user shared a news article about The Greens that contained a photograph of Glawischnig-Piesczek. As part of a comment to this article, the user accused Eva Glawischnig-Piesczek of being a member of a “fascist party”, a “corrupt oaf” and a “traitor to her people” (“Volkverräterin”), an insult that was used by the Nazis.

Eva Glawischnig-Piesczek could not sue the author of the insults, who had used a false user name. She therefore asked Facebook to remove the offensive comment, which was defamatory in her view. Since the social media platform did not comply with this request, Glawischnig-Piesczek brought an action before the competent national court.

---


It is a matter of national law to determine whether a statement is defamatory. The Austrian courts of first and second instance and the Austrian Supreme Court (Oberster Gerichtshof) found that the online comment at issue was defamatory under Austrian law. They based their decisions on paragraph 1330 of the General Civil Code (ABGB), which provides for compensation for defamation, as well as on paragraph 78 of the Law on Copyright (Urheberrechtsgesetz), which protects the right to one’s image. According to the Supreme Court, these provisions were violated because the comment contained general statements that were harmful to Glawischning-Piesczek’s reputation, as opposed to specific criticism based on some sort of verifiable evidence.

The EU law questions raised by the dispute related to the interpretation of the eCommerce Directive. Section 4 (of Chapter II) of the eCommerce Directive restricts the liability of providers of information society services that serve as intermediaries. Intermediaries engage in “mere conduit” (Art. 12), “caching” (Art. 13) or “hosting” (Art. 14) of content generated by their users. They are exempted from secondary liability for their users’ unlawful activities under the conditions specified in Articles 12 to 14 of the eCommerce Directive. The secondary liability exemption of intermediaries is justified by their function as “communication enablers”.

In addition to the secondary liability exemption, Section 4 of the eCommerce Directive precludes general obligations that require intermediaries to monitor users’ content. Article 15(1) of the eCommerce Directive provides:

“Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.”

In the proceedings before the Austrian Supreme Court, it was undisputed that Facebook was a host provider in the sense of Article 16 of the Austrian eCommerce Law, which transposed Article 14 of the eCommerce Directive. This meant that Member States were precluded from imposing general monitoring obligations on the social media platform.

7. Ibid., section 2.
9. 6 Ob 116/17b, 3.2, 3.4.
However, the Austrian Supreme Court had doubts regarding the meaning and scope of Article 15(1) of the eCommerce Directive. It did not know what kinds of injunctions a national court could impose on a host provider such as Facebook without violating the prohibition of general monitoring obligations. It was clear that a national court could not impose “obligations of a general nature”, as Recital 47 of the eCommerce Directive confirms. However, Recital 47 also states that “this does not concern monitoring obligations in a specific case”. Moreover, according to Article 14 of the eCommerce Directive, the liability exemption stipulated in this provision does not hinder national courts from imposing cease and desist orders in accordance with national law. Hence, the Austrian Supreme Court needed to know whether the obligations that were at issue in this case were of a general nature and thus prohibited, or of a specific nature and thus permitted.

The difficulty in this case was that the injunction envisaged required Facebook not only to remove the insulting comment that was held to be defamatory, but also to remove any content on the platform that was identical or equivalent to this comment. In order to identify and remove identical and equivalent content, the host provider would have to engage in some sort of content monitoring. For this reason, the Austrian Supreme Court doubted whether such an injunction was compatible with the prohibition of general monitoring obligations of Article 15(1) of the eCommerce Directive. It therefore asked the ECJ to interpret this provision.

In essence, the Austrian Supreme Court asked for three clarifications. First, it sought to find out whether a cease and desist order could be extended to other content hosted by the provider, if this content was identical to the statement which was held to be defamatory by a court. Second, the Supreme Court asked whether such a court order could be extended to statements that have a meaning that is equivalent to that of the defamatory statement. Third, the Supreme Court asked whether an obligation to remove or block identical and/or equivalent content could be imposed worldwide.

3. Opinion of the Advocate General

Advocate General Szpunar delivered his Opinion in June 2019. Before proposing answers to the preliminary questions, he gave his own interpretation of identical and equivalent content. The Advocate General understood identical content as a precise manual reproduction of the information that was characterized as illegal and as an automated
reproduction, made through the “share” function.\textsuperscript{11} The term equivalent content, the Advocate General pointed out, gave rise to difficulties of interpretation. The preliminary reference suggested it was content that “scarcely diverges from the original information” or content whose message “remains essentially unaltered”.\textsuperscript{12} The Advocate General understood equivalent content as “reproduction of the information that was characterized as illegal containing a typographical error and a reproduction having slightly altered syntax or punctuation”.\textsuperscript{13} Thus, he provided a narrow interpretation of equivalent content. However, he admitted that equivalence might go further than such cases.\textsuperscript{14}

The Advocate General’s position differed in relation to identical or equivalent content. He found that a host provider may be ordered to identify identical content for the purpose of enforcing an injunction.\textsuperscript{15} If a specific infringement had already been identified, the obligation to identify identical content by the same user did not constitute a general monitoring obligation.\textsuperscript{16} The Advocate General applied the same reasoning to identical information disseminated by other users, since the injunction would still be targeted at a specific infringement.\textsuperscript{17} Moreover, he observed that identical content by any user seemed “capable of being detected with the help of software tools, without the host provider being obliged to employ active non-automatic filtering of all the information disseminated via its platform”.\textsuperscript{18} For the same reason, the obligation did not entail an excessive breach of the right to freedom to conduct a business (Art. 16 EU Charter of Fundamental Rights).\textsuperscript{19}

In addition, an injunction requiring monitoring of identical content respected internet users’ fundamental right to freedom of expression and information (Art. 11 of the Charter) as this right had to be weighed against the protection of other fundamental rights.\textsuperscript{20} The Advocate General also took into account that such an injunction might result in the removal of content by users other than the original perpetrator. Interestingly, he proposed that third parties who are affected by the injunction should be able to challenge, before a court, the implementing measures adopted by a host provider on the basis of the

\textsuperscript{11} Ibid., para 56.
\textsuperscript{12} Ibid., para 67.
\textsuperscript{13} Ibid.
\textsuperscript{14} Ibid.
\textsuperscript{15} Ibid., para 57.
\textsuperscript{16} Ibid., para 58.
\textsuperscript{17} Ibid., paras. 59–60.
\textsuperscript{18} Ibid., para 61.
\textsuperscript{19} Ibid., para 63.
\textsuperscript{20} Ibid., para 65.
injunction, and that possibility must not be conditional on being a party to main proceedings.\textsuperscript{21}

Regarding equivalent content, the Advocate General stated that a host provider may be ordered to identify content equivalent to that found to be illegal when it originates from the same user.\textsuperscript{22} He based his opinion on the 2011 judgment in \textit{L'Oréal v. eBay}, in which the ECJ had stated that injunctions can be issued not only to bring infringements to an end, but also to prevent further infringements.\textsuperscript{23} According to \textit{L'Oréal v. eBay}, an intermediary can be ordered to suspend the perpetrator of an intellectual property infringement in order to prevent further infringements of that kind by the same seller in respect of the same trade marks.\textsuperscript{24} However, the ECJ had made clear in \textit{L'Oréal v. eBay} that the prevention of further infringements could not be achieved through an active monitoring of all the data of each user of the intermediary.\textsuperscript{25}

Addressing the effect on fundamental rights, the Advocate General observed that the obligation to identify equivalent content by the same user must “respect the principle of legal certainty and ensure that the effects of that injunction are clear, precise and foreseeable”.\textsuperscript{26} Therefore, the court issuing the order had to weigh up the fundamental rights involved and take account of the principle of proportionality.

The Advocate General expressed a different opinion, however, in relation to equivalent content originating from different users. Identification of such content would require the monitoring of all the information disseminated via a social media platform and would therefore amount to prohibited general monitoring. Unlike identical content, equivalent content could only be identified if an intermediary employed sophisticated monitoring solutions.\textsuperscript{27} As a result, “not only would the role of a service provider carrying out general monitoring no longer be neutral, in the sense that it would not be merely technical, automatic and passive, but that service provider, by exercising a form of censorship, would become an active contributor to that platform”.\textsuperscript{28}

Further, an obligation to identify equivalent content from any user would not ensure a fair balance between the fundamental rights involved. On the one

\textsuperscript{21} Ibid.
\textsuperscript{22} Ibid., para 72.
\textsuperscript{23} Case C-324/09, \textit{L’Oréal SA and Others v. eBay International AG and Others}, EU:C:2011:474, para 144.
\textsuperscript{24} Ibid., para 141. See also Case C-494/15, \textit{Tommy Hilfiger Licensing LLC and Others v. DELTA CENTER a.s.}, EU:C:2016:528.
\textsuperscript{25} Case C-324/09, \textit{L’Oréal v. eBay}, para 139.
\textsuperscript{26} Opinion, para 71.
\textsuperscript{27} Ibid., para 73.
\textsuperscript{28} Ibid.
hand, it would require costly solutions by the intermediaries; on the other hand, it would lead to censorship and thus to systematic restrictions of freedom of expression and information.29

To sum up, the Advocate General suggested that a national court could order a host provider to identify and remove identical content generated by any user and equivalent content generated by the same user. In terms of the effect on fundamental rights, he considered that monitoring obligations for identical content by any user would not be disproportionate to the right to freedom of expression or the right to freedom to conduct a business. However, monitoring obligations for equivalent content by the same user might have adverse consequences for the fundamental rights at issue; therefore, the order must consider fundamental rights and the principle of proportionality. Monitoring obligations for equivalent content by any user would lead to disproportionate fundamental rights violations.

4. Judgment of the Court

The ECJ judgment followed the Opinion of the Advocate General only partially. Regarding identical content, the ECJ ruled that the eCommerce Directive did not preclude national courts from ordering removals or blocking of information that is identical to information that has previously been declared to be unlawful, irrespective of who requested the storage of that information.30 The ECJ, therefore, agreed with the Advocate General that an injunction to remove identical content could target content posted by any user of the hosting service.

However, the ECJ did not follow the Advocate General’s Opinion regarding equivalent content. It ruled that the eCommerce Directive did not preclude national courts from ordering removals or blocking of information that is equivalent to information that has previously been declared to be unlawful.31 In the Court’s opinion, for the injunction to be effective, it must extend to information that is “worded slightly differently, because of the words used or their combination”, “whilst essentially conveying the same message”.32 Unlike the Advocate General, the ECJ did not limit the scope of the permitted injunction to content originating from the same user, meaning that it could extend to equivalent content originating from any user.

29. Ibid., para 74.
31. Ibid., paras. 38–41.
32. Ibid., para 41.
To avoid an excessive obligation being imposed on the host provider, the equivalent content must be properly identified in the injunction. In any event, the host provider cannot be required to carry out an independent assessment of the content due to differences in the wording between the original and the equivalent content. Provided that these requirements are fulfilled, an injunction that extends to equivalent content did not impose a general monitoring obligation, or a general obligation to actively seek facts or circumstances indicating illegal activity in the sense of Article 15(1) of the eCommerce Directive.

As a third point, the ECJ ruled that the eCommerce Directive did not preclude such an injunction from producing effects worldwide. As the Court explained, the Directive did not provide for any limitation, including a territorial limitation, on the scope of the measures that Member States were entitled to adopt. Referencing Recitals 58 and 60 of the eCommerce Directive, however, the ECJ highlighted that EU rules in the area of electronic commerce were consistent with the rules applicable at international level. It was up to Member States to ensure that the measures which they adopt and which produce effects worldwide take due account of those rules.

5. Comment

This comment is divided into three sections. Section 5.1 examines the ECJ’s interpretation of the prohibition of general monitoring obligations. Section 5.2 looks at implications of injunctions such as the one at issue in this case for the fundamental right to freedom of expression and information. Section 5.3 discusses the territorial scope that such injunctions may be given.

5.1. General monitoring v. specific monitoring

The central question in Glawischnig-Piesczek was whether an injunction that required an intermediary to remove online content that was identical or equivalent to content that was previously held to be unlawful amounted to general as opposed to specific monitoring. As mentioned above, Article 15(1)
of the eCommerce Directive precludes general monitoring obligations, but it permits specific monitoring obligations in Glawischnig-Piesczek.39

Section 5.1.1 below demonstrates that in Glawischnig-Piesczek the ECJ departed from its previous understanding of general monitoring. Section 5.1.2 argues that this new approach was motivated by the Court’s intention to ensure the effectiveness of national injunctions against illegal online content. At the same time, the ECJ made clear that national injunctions cannot impose an excessive burden on intermediaries. As shown in Section 5.1.3, in the Court’s opinion, national injunctions could lead to prohibited general monitoring if the intermediary has to carry out an independent assessment of the content at issue. The Court assumed that intermediaries could employ automated tools and technologies in order to identify identical or equivalent content. Section 5.1.4 focuses on the automated search of illegal online content.

5.1.1. Departure from prior criteria
Before Glawischnig-Piesczek, the ECJ had distinguished general from specific monitoring in a number of judgments regarding infringements of intellectual property rights. Two criteria resulted from the previous case law. First, the ECJ defined general monitoring as monitoring of all the data transmitted on the digital platform. Second, the ECJ suggested that monitoring was permissible if it was restricted to a specific perpetrator who had already engaged in an illegal activity.

Regarding the first criterion, the ECJ repeatedly stated that it followed from Article 15(1) of the eCommerce Directive that an intermediary cannot be obliged “to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual property rights”.40 In other words, an intermediary carries out general monitoring, if it observes almost all the information that it transmits and all users of its service.41

Arguably, this understanding of general monitoring entailed that an intermediary could not be required to scan all the data files it stored in order to identify certain specific files. In his Opinion in UPC Telekabel Wien, Advocate General Cruz Villalón argued that it would be incompatible with Article 15(1) of the eCommerce Directive if an intermediary was ordered “to filter all the data carried in its network in order to ascertain whether they

39. See supra section 2.
40. Case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771, para 36. See also Case C-324/09, L’Oréal v. eBay, para 139; Case C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, EU:C:2012:85, para 34.
41. Case C-70/10, Scarlet Extended, para 39; Case C-360/10, SABAM, para 37; Case C-484/14, Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, EU:C:2016:689, para 87.
constitute transfers of specific protected film works and to block such transfers”.42

As a second criterion, the ECJ indicated in its case law preceding Glawischnig-Piesczek that monitoring was permissible if it was restricted to infringements of the same nature by the same infringer. In particular, it found in L’Oréal v. eBay that the operator of an online marketplace can be ordered by means of an injunction to prevent further infringements of the same kind by the same seller in respect of the same trade marks.43 In an offline context, Tommy Hilfiger confirmed that permissible specific monitoring is limited to “avoiding new infringements of the same nature by the same market-trader from taking place”.44 Courts could not require “general and permanent oversight” over all customers.45 According to Husovec’s interpretation of this case law, an intermediary could be obliged to prevent repeat infringements by the same infringer, but it could not be obliged to prevent reappearance of unlawful content from anyone.46

However, in Glawischnig-Piesczek, the ECJ did not apply the two criteria it had developed in its previous case law. If it had applied the first criterion, it would have examined whether the injunction at issue required the intermediary to monitor all the data of all of its customers. Since all the content of all customers has to be scanned to identify identical and equivalent content, the injunction would probably have been incompatible with the first criterion. Furthermore, if the ECJ had adhered to the second criterion, it would have restricted the monitoring to content by the same perpetrator.

Instead, the ECJ held that Article 15(1) of the eCommerce Directive does not prevent a national court from obliging an intermediary to remove or block identical or equivalent content.47 It did not matter that the intermediary would have to search through all the uploads of all its users to comply with this obligation. The Court specifically found that intermediaries could be requested to remove or block identical and equivalent content irrespective of who generated this content.48 The injunction did not have to be limited to content by the same user; it could extend to content by any user.

43. Case C-324/09, L’Oréal v. eBay, para 141. See Section 3 above for a discussion of this case by A.G. Szpunar.
44. Case C-494/15, Tommy Hilfiger, para 34; Husovec, Injunctions against intermediaries in the European Union: Accountable but not liable? (Cambridge University Press, 2017), p. 120.
45. Case C-494/15, Tommy Hilfiger, para 34.
46. Husovec, op. cit. supra note 44, p. 121.
48. Ibid., para 37.
Thus, the ECJ ignored its longstanding understanding of general monitoring and it departed from its earlier position, according to which injunctions could be targeted only at repeat infringements by the same infringer.49 Unfortunately, the Court failed to distinguish its new approach from its prior approach. In fact, it did not mention or engage with its previous case law at all.

What distinguishes the Glawischnig-Piesczek judgment from the previous case law on Article 15(1) of the eCommerce Directive is that it did not concern intellectual property rights, but an individual’s personality right not to be defamed. This difference could explain why the ECJ opted for a new approach and provided stronger protection from the proliferation of illegal online content. The Court apparently found it more important to protect the integrity of victims of online defamation than the commercial interests of holders of intellectual property rights.

It would indeed make sense to take the weight of the interest to be protected into account when determining the monitoring duty that may be lawfully placed on an intermediary. In future cases, the ECJ could reconcile its prior approach with the present judgment by taking into account the different rights and interests at stake when interpreting Article 15(1) of the eCommerce Directive. As we will see in section 5.1.3 below, the Court’s new approach to Article 15(1) includes an assessment of the proportionality of the obligation imposed on the intermediary. The weight of the interest to be protected could and should be considered in this balancing exercise.

The departure from the previous case law in Glawischnig-Piesczek might also be linked to the increased awareness of the perils of user-generated online content that marks recent policy initiatives at the EU and at the national level. As mentioned in the introduction above, the EU legislature has introduced new monitoring responsibilities for intermediaries regarding copyrighted content and terrorist content and it is planning to revise the general liability regime for intermediaries with the new Digital Services Act. Moreover, the European Commission has adopted soft law instruments that aim to prevent and counter the spread of hate speech and disinformation, and it continuously evaluates their impact.50 At the national level, Germany has adopted legislation that obliges social media platforms to set up an effective and transparent mechanism for complaints against illegal online content and to

49. See also Keller, “Facebook filters, fundamental rights, and the CJEU’s Glawischnig-Piesczek ruling”, (2020) *GRUR International*, 1–8 (advance article), at 5.

delete this content within specific timeframes.\textsuperscript{51} It is possible that these developments encouraged the Court to improve the protection from illegal online content by means of judicial interpretation.

5.1.2. \textit{Sufficiently effective national injunctions}

The ECJ’s interpretation of Article 15(1) of the eCommerce Directive relied on two lines of reasoning, which will be discussed in this section and the next one (5.1.3), respectively. The first line of reasoning was based on a systematic analysis of Article 15(1). The Court’s main argument in this regard was that the Directive recognized the importance of effective national injunctions that are aimed at ending unlawful activities online. In particular, the ECJ emphasized that Article 14 of the eCommerce Directive, read in conjunction with Recital 45, is intended to exempt host providers from liability where they satisfy one of the two conditions listed in that provision, but does not shield them from injunctions based on national law.\textsuperscript{52}

Furthermore, according to Article 18 of the eCommerce Directive, Member States had to ensure that national court actions concerning activities of information society services “allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved”.\textsuperscript{53} In several of its language versions, albeit not in the German one, this provision explicitly demanded the termination of “any” infringement and the prevention of “any” further impairment.\textsuperscript{54} The ECJ also recalled Recital 52 of the eCommerce Directive, which indicates that appropriate court actions are necessary since “damage which may arise in connection with information society services is characterized by both its rapidity and by its geographical extent”.\textsuperscript{55} The Court derived from these provisions that Member States had a “particularly broad discretion” regarding domestic court actions.\textsuperscript{56}

The ECJ’s systematic analysis of Article 15(1) of the eCommerce Directive is convincing. Overall, the Directive indeed recognizes that interim measures adopted by national courts are necessary to address swiftly any negative consequences that the activities of information society services may have. Moreover, the wording of Article 18 of the Directive suggests that Member States are under an obligation to provide for court actions that do not only

\textsuperscript{51} Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz, NetzDG), BGBl. I 2017, 3352.
\textsuperscript{52} Judgment, paras. 23–25.
\textsuperscript{53} Ibid., para 26.
\textsuperscript{54} Ibid., para 30.
\textsuperscript{55} Ibid., para 28.
\textsuperscript{56} Ibid., para 29.
bring infringements to an end, but also prevent any further adverse effects on the interests at stake.

The ECJ’s specific answers to the Austrian Supreme Court’s questions were guided by this interpretation of Article 15(1) of the eCommerce Directive. They were based on the premise that national injunctions aimed at terminating an illegal online act and preventing it from being repeated should be effective.

Regarding identical content, the ECJ found that it was legitimate for a national court to order the blocking or removal of content, which is identical to content previously declared to be illegal, “irrespective of who requested the storage of that information”.57 Otherwise, further impairment of the interests involved would not be prevented. When evaluating the risk of further impairment, the ECJ took into account the workings of social networks: “Given that a social network facilitates the swift flow of information stored by the host provider between its different users, there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network.”58

The ECJ was right to find that the effectiveness of the injunction would be drastically reduced if it was limited to the specific comment that was found to be defamatory. As the Court acknowledged, content on social networks tends to be further disseminated by other users, which entails that victims of unlawful comments would have to bring multiple court actions in respect of each comment that is identical to the original one. Neither would it be a viable alternative to restrict the injunction to identical content by the same perpetrator.59 It would be too easy to circumvent the injunction by creating a new account on the social media platform under a different name. As mentioned above, the insulting comment in the case at issue was written by a user who had used a false user name and could not be identified.

For a similar reason, the ECJ found that an injunction such as the one at issue must be able to extend to equivalent content in order to be effective.60 The ECJ agreed with the Austrian Supreme Court that the injunction could otherwise “easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal”.61 For the person concerned, this could mean that he or she has to bring multiple proceedings to bring an end to the illegal conduct. Thus, the injunction would not provide sufficiently effective protection for the victim, if it was not

57. Ibid., para 37.
58. Ibid., para 36.
59. Opinion, para 71.
60. See judgment, para 41.
61. Ibid.
extended to equivalent content. It is to be welcomed that the Court strove to promote the effectiveness of national injunctions aimed at ending illegal activities online and that it considered the actual workings of social networks in this endeavour.

The ECJ’s approach is in line with a longstanding principle of Austrian procedural law. The Austrian Supreme Court has continuously held that cease and desist orders in general do not have to be restricted to acts that are identical; they can be extended to all acts that are similar in their core. The aim of this principle is to avoid the perpetrator being able to circumvent the cease and desist order by engaging in an activity that is not identical, but very similar to the unlawful activity that is targeted by the order.

In Germany, a similar principle is known as Kerntheorie (“core theory”). The German Kerntheorie is linked to Störerhaftung, a special notion of “disturbance liability” for interim relief that was created by German courts. Störerhaftung is applied in the online context to impose injunctions on intermediaries for intellectual property rights infringements by their users. The doctrine allows the issuance of cease and desist orders not only to the immediate wrongdoer and any participant in the wrongdoing, but also the so-called “disturbers” (Störer). Such disturbers are the parties that deliberately, adequately and causally contribute to an infringement by others. The disturber, moreover, must have either the legal or the factual

62. See ibid., para 46.
64. 6 Ob 116/17b, section 3.1.
66. Störerhaftung is a judicial creation. In Germany, injunctive relief is not explicitly provided by the tort provisions of the Bürgerliches Gesetzbuch (BGB), but it has been made available by analogy to the law of property. Störerhaftung finds its roots in the property defence claims laid out in Articles 862 and 1004 BGB, which enable injunctive relief essentially against cases of nuisance. See Angelopoulos, European intermediary liability in copyright: A tort-based analysis (Kluwer Law International, 2016), p. 150; Opinion of A.G. Jääskinen in Case C-324/09, L’Oréal SA and Others v. eBay International AG and Others, EU:C:2010:757, para 56; Bornkamm, “E-Commerce Directive vs. IP rights enforcement – Legal balance achieved?”, (2007) Gewerblicher Rechtsschutz und Urheberrecht (GRUR), 642.
67. Angelopoulos, op. cit. previous note, p. 151.
possibility to terminate the infringement by a third party.68 An injunction can be imposed if the disturber ignored the duty to review (Prüfungspflicht).69

Kerntheorie implies that the duty to review does not apply only to identical copies of the content, or to copies uploaded by the same users; the duty actually extends to all subsequent infringing acts of a similar nature that are easily recognizable.70 In short, the infringements must be “similar in their core” (“Kern”).71 Thus, in Germany, intermediaries can be obliged through an injunction to remove or block specifically defined online content that infringes copyright and the obligation can be extended to any content that leads to infringements that are similar in their core. After receiving a notification, the host provider is expected to block and remove obvious re-postings without waiting for a new notification.

It is easy to see the analogy of the Austrian and German approaches with the Glawischnig-Piesczek ruling. The ECJ permitted national injunctions to be extended to equivalent content; Austrian and German courts have continuously extended injunctions to content whose dissemination would lead to infringements that are similar in their core. For this reason, the first German-language comments on the Glawischnig-Piesczek ruling did not express much surprise about the possibility to extend injunctions to equivalent content.72

Previously, the extension of injunctions – in the German-speaking Member States – to similar infringements had been criticized in the academic literature for stretching the interpretation of Article 15(1) of the eCommerce Directive too far by labelling general monitoring as specific. It was argued that a judge-made “notice and stay down” regime was created if the purpose of an injunction was not only to counter a specific infringement, but to prevent future similar infringements. This “notice and stay down” regime, so the argument went, was more extensive than the “notice and take down” regime provided by the eCommerce Directive. Therefore, German courts were sometimes accused of misconceiving the main goals that the EU legislature

70. Bornkamm, op. cit. supra note 66.
pursued when drafting the eCommerce Directive. However, the German approach has now been vindicated by the ECJ.

5.1.3. No excessive obligation for the intermediary
As we have seen in the previous section, the ECJ’s first line of reasoning in *Glawischnig-Piesczek* consisted of emphasizing the importance of effective national injunctions, following the example of German and Austrian courts. The second line of reasoning concerned the proportionality of the obligation imposed on the intermediary. In the view of the Court, Article 15(1) of the eCommerce Directive “implies that the objective of an injunction . . . may not be pursued by imposing an excessive obligation on the host provider”. Although the Court does not use the term proportionality, it seems to suggest that a kind of balancing exercise has to take place. The ECJ derived this rule from a purposive interpretation of Article 15(1) of the eCommerce Directive. It noted that the “EU legislature wished to strike a balance between different interests at stake” when it adopted the Directive. For the Court, this was apparent from Recital 41 of the Directive.

*Glawischnig-Piesczek* was actually the first case in which the ECJ interpreted Article 15(1) of the eCommerce Directive in this way. As we mentioned above, in its previous case law, the Court repeated the mantra that Article 15(1) excludes obligations that require intermediaries to monitor all the data of all of their users. The fact that the ECJ did not do so in the present case could mean that it has abandoned this rigid requirement, opting for a more flexible, purposive interpretation of Article 15(1) instead. We have shown above that this purposive interpretation of Article 51(1) makes it possible to weigh different rights and interests against each other.

By ignoring its own strict rule that intermediaries cannot be required to monitor all the data of all their customers, the ECJ also opened the door for a future reconciliation of the eCommerce Directive and the recently adopted specific legislation that stipulates monitoring obligations for certain types of online content. Most likely, the ECJ will eventually be asked to interpret Article 17 of the DSM Directive, which imposes monitoring obligations on intermediaries for copyrighted material. Article 17 is *lex specialis* to Article 14 of the eCommerce Directive; it introduces an exception to the liability

73. For a comprehensive account of the criticism of the German approach, see Angelopoulos, op. cit. supra note 66, Ch. 3, section 3.3.1.3.
74. See judgment, para 44.
75. Ibid., para 43.
76. See supra section 5.1.1.
exemption for host providers. However, the DSM Directive has not abolished the prohibition of general monitoring obligations for copyrighted material. Article 17(8) of the DSM Directive re-emphasizes that this article shall not lead to any general monitoring obligation. Under the ECJ’s case law that preceded Glawischnig-Piesczek, the obligations imposed by Article 17(4) would amount to general monitoring and there would therefore be an internal contradiction within Article 17.

The proposed Terrorist Content Regulation has the same inherent conflict. It provides that intermediaries should take “proactive measures to protect their services against the dissemination of terrorist content”. At the same time, the measures should not lead to general monitoring obligations. The ongoing discussions on the Digital Services Act suggest that the Commission is also planning to maintain the current prohibition of general monitoring obligations in this piece of legislation.

In a future ruling, the ECJ could reconcile the conflicting requirements through a purposive interpretation of general monitoring that balances the different interests at stake. In this balancing exercise, it could take into consideration that monitoring obligations might be proportionate for intermediaries such as Facebook, but excessive for intermediaries with fewer resources. The disadvantage of this approach when compared to a strict rule is that the definition of general monitoring is no longer stable, which decreases legal certainty. Moreover, there is a risk that the general monitoring prohibition might be eroded and made meaningless if it is interpreted too restrictively in the future. However, in this regard, the significance of Glawischnig-Piesczek should not be overstated. It is important to note that the ECJ’s interpretation of general monitoring in this case is tied to the specific context of injunctions.

On the specific case of injunctions, the ECJ found in Glawischnig-Piesczek that an injunction would impose an excessive burden on the intermediary, if it required it to carry out an independent assessment of the content at issue. To
avoid the intermediary having to carry out an independent assessment, the injunction had to fulfil certain requirements. It was important, according to the Court, that the injunction specified: a) the name of the person concerned; b) the circumstances in which the infringement was determined; and c) “equivalent content to that which was declared to be illegal”. These caveats demonstrate that the Court was mindful of the general monitoring prohibition of Article 15(1) of the eCommerce Directive.

The ECJ defined equivalent content as content that conveyed a message that remained “essentially unchanged” and therefore diverged “very little” from the original content. The Court explained that equivalent content was content that conveyed the same illegal message, although it was “worded slightly differently because of the words used or their combination” differed.

This definition of equivalent content is broader than information “containing a typographical error and a reproduction having slightly altered syntax or punctuation” used by the Advocate General. While the Advocate General focused on spelling, word order or punctuation, altering of which is often used to mislead automated filters, the Court seemed to include messages containing different wording. As a result, in this particular case, Facebook would be required to delete content that uses other words to imply that Eva Glawischnig-Piesczek is corrupt, fascist or a traitor to her people. It is not clear, however, how far the rephrasing could go for the message to still be considered essentially the same. It will be for the Austrian Supreme Court to resolve this puzzle. In any event, the injunction should not be understood as an open-end order to catch any kind of insult of the person requesting the injunction.

Moreover, the ECJ left it open how the national court should specify content that is equivalent to the original defamatory content. Would it have to come up with a list of comments that are “equivalently” illegal? This would limit the injunction to particular wording or phrasing. The intermediary would not have to foresee the unlimited possibilities of alternative phrasing. Such a list would blur the distinction between “equivalent” and “identical” content, as both must be identified in advance with sufficient specificity to allow a machine to reliably, without human supervision, carry out a court’s order.

However, such an injunction might be circumvented by using formulations that are not listed in the injunction. One could imagine that for a creative master of insults the possibilities are endless. Alternatively, will the national
court have to explain in detail what it is that made the original content illegal? This would make it more difficult to circumvent the injunction, but it would require some sort of assessment by the intermediary.

The ECJ left it to the national judiciary to determine the equivalent content that is covered by the injunction. This lack of legal certainty will inevitably lead to disputes about the classification of content as equivalent. The question remains, moreover, if the limitations installed by the ECJ will be followed with regard to the specificity by the national courts issuing the actual injunctions.

5.1.4. “Recourse to automated search tools and technologies”
In one of the most striking passages of the judgment, the ECJ declared that an obligation to identify equivalent content is not excessive, if it does not “require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies”. According to the French version of this passage, the obligation is not excessive providing it “n’oblige pas l’hébergeur à procéder à une appréciation autonome, ce dernier pouvant, ainsi, recourir à des techniques et à des moyens de recherche automatisés”. This seems to imply that intermediaries can be obliged to remove or block equivalent content only insofar as they are able to do so by automated means. Apparently, they cannot be obliged to include human content moderators in this process. However, the meaning of this passage is not entirely clear and it will have to be substantiated by the ECJ in future cases.

It seems that the ECJ chose this approach to avoid the risk pointed out by the Advocate General; namely, that too much involvement of the host provider in the monitoring process could lead to the loss of immunity provided by Article 14 of the eCommerce Directive. After all, human assessment could be interpreted as a form of active hosting leading to (at least constructive) knowledge of illegality. Similarly to the ECJ, the Advocate General distinguished between software tools and “active non-automatic filtering”. According to the Advocate General, employing software tools would not lead to general monitoring, whereas active non-automatic filtering would have such an effect.

Nevertheless, eliminating human assessment from the monitoring process is somewhat surprising, to say the least. Detecting content that is identical or

85. Spindler, op. cit. supra note 72, at 3275.
86. Judgment, para 46.
87. Ibid.
88. See also Spindler, op. cit. supra note 72; Keller, op. cit. supra note 84.
89. Judgment, para 46.
90. Opinion, para 71.
equivalent by using automated search tools is actually not as easy as the ECJ seems to assume.

Automated detection of content is difficult even if the content is specifically listed in the injunction. If the intermediary has to identify identical content or equivalent content that is specifically formulated in the injunction, it could employ automated filters that rely on the detection of duplicates. Duplicate detection can be used to identify identical and equivalent content that is already on the platform as well as to prevent new content of this kind being uploaded. As explained in the Annex to the Impact Assessment for the DSM Directive, such an upload filter would rely on “fingerprinting”, i.e. on databases of all fingerprinted content against which every newly uploaded piece of content is checked. If there is a match, the new content is removed or access to it is blocked. The Annex gives the example of YouTube’s Content ID system, which controls every new video uploaded to the platform.91

Yet, duplicate detection tools are error-prone when they are meant to identify illegal text such as hate speech or defamation since the same words can be illegal in one context and legal in another.92 As we will demonstrate in section 5.2.2 below, a phrase that constitutes illegal hate speech or defamation could be lawful if it used in a different context, for example for journalistic reporting, scholarly analysis, education or awareness raising. For this reason, duplicate detection filters tend to be used more often for images and videos than for text.93 Child pornography is an example of content that is identified by automated upload filters before it is disseminated on the platform.94 Platforms also use automated filters to identify images or videos that were classified as terrorist content.95 Automated filters tend to be used less often for the identification of hate speech or defamation. Rather than on automated detection, many platforms currently rely on a reporting system to detect hate

---

94. Ibid., at 1636.
speech and defamation. Illegal content is reported (“flagged”) by other users and reviewed by human content moderators against internal guidelines.96

If the equivalent content is not specifically formulated in the injunction, automated detection is even more difficult. Any tool to detect this content would not be doing a mere comparison of texts, but would actually have to classify content as belonging to the category of equivalent content or not.97 The existing Artificial Intelligence systems are not yet sophisticated enough to do so reliably.98 The Impact Assessment to the proposed Terrorist Content Regulation admits that language processing systems (which were proposed in that instrument) are “immature for accurately identifying illegal hate speech or other violent speech.”99 There is no indication that detection of defamatory content would be any more successful than detection of hate speech. This is particularly problematic from a fundamental rights perspective, as section 5.2 below will show.

In addition, Facebook would not only have to automatically identify identical and equivalent content, it would also have to use face recognition techniques to identify all pictures saved on the platform that show Eva Glawischnig-Piesczek. In the original defamatory Facebook posting, the name Glawischnig was not mentioned. The insults were made in a comment to a news article about The Greens that contained a picture of Eva Glawischign. However, in the current state of the art, face recognition tools are still prone to error as they lead to false positives and negatives. While humans can recognize faces that vary in pose, illumination and facial expression, this task is still very challenging for machines.100

Rather than categorically excluding human review, the ECJ should have taken into account the current state of the art of automated search tools and

96. Klonick, op. cit., supra note 93, at 1638.
technologies and the actual practice of platforms such as Facebook. Alternatively, it could have invited the referring court to do so. Hopefully, the ECJ will clarify in subsequent case law that it did not wish to imply in Glawischnig-Piesczek that intermediaries can only be obliged to remove or block content if they can do so by automated means.

5.2. Implications for the right to freedom of expression and information

5.2.1. Absence of any fundamental rights review

In Glawischning-Piesczek, the ECJ declared that injunctions that require intermediaries to block or remove identical and equivalent content are compatible with Article 15(1) of the eCommerce Directive. The Court mentioned that these injunctions had to be proportionate, but only with regard to the obligation imposed on the intermediary. It did not address the potential implications of the injunctions on the fundamental rights of other interested parties. Hence, it ignored their potential adverse effect on third parties that might be affected.

The Austrian courts apply Articles 15 and 18 of the eCommerce Directive when they impose injunctions on an intermediary such as Facebook. This means that the case falls within the scope of application of the Charter of Fundamental Rights, as defined in Article 51(1) of the Charter. Nevertheless, the ECJ chose not to provide any additional guidance on the possible implications of broad injunctions on the fundamental rights protected by the Charter and left this assessment entirely to the Austrian Supreme Court.

Admittedly, the three questions referred to the Court did not specifically address the fundamental rights aspect. However, the absence of any fundamental rights considerations is a missed opportunity as the judgment could have served as a benchmark for rights-compatible practices of the moderation of online content. It is surprising that the ECJ did not use this opportunity since it had done a fundamental rights balancing exercise in earlier judgments such as Scarlet Extended.101 Moreover, in his Opinion, Advocate General Szpunar discussed at length how an adequate balance between the different fundamental rights could be achieved.102

Above all, injunctions such as the ones at issue in this case might pose risks to the right to freedom of expression and information, which is enshrined in Article 11 of the Charter. It is clear that any injunction ordering removal or blocking access to content interferes with speech of users of a service, of those who want to express their opinions and those who merely want to access this information, but possibly also of the service provider itself.

101. Case C-70/10, Scarlet Extended, para 41; Case C-360/10, SABAM, para 39.
The right to freedom of expression and information is not absolute. Under Article 52 of the Charter, limitations may be possible if they are proportionate and necessary and genuinely meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others. There is no doubt that the extension of the relevant injunction to identical and equivalent content aimed to protect the rights and freedoms of others, namely Eva Glawischnig-Piesczek’s personality rights.

The analysis below focuses on the implications of injunctions to remove identical and equivalent content on freedom of expression and information. As pointed out by Keller, the judgment may also raise concerns about the right to the protection of personal data (Art. 8 of the Charter), the right to a fair trial and an effective remedy (Art. 47 of the Charter) and the right to equality and non-discrimination (Art. 21 of the Charter) since algorithmic filters have been found to discriminate against members of minorities or marginalized racial or linguistic groups.\(^{103}\) The injunction needs to be implemented at the national level in a way that avoids disproportionate infringements of these rights. Besides, the intermediary’s interests could be framed as elements of the freedom to conduct a business (Art. 16 of the Charter), as the Advocate General did in his Opinion. However, the previous use of this right by the ECJ has sometimes been criticized and it is doubtful whether much can be gained by framing intermediaries’ business interests as fundamental rights.\(^{104}\)

5.2.2. Context sensitivity

There are several elements of the judgment that suggest that the interference with the right to freedom of expression and information might not be proportionate, unless it is accompanied by appropriate safeguards. Overall, these aspects relate to the fact that the same content might be viewed differently depending on the context in which it is used.

The ECJ rightly assumed that there was a genuine risk of information, which was held to be illegal, being subsequently reproduced and shared. In the view of the Court, it was therefore legitimate for a national court to require the host provider to remove or block access to identical or equivalent content. However, even identical content could be used in a different context or for a different purpose, for example for journalistic reporting, scholarly analysis, education or for raising awareness.\(^{105}\) New, legitimate uses of the same content

---

105. Some examples of removal of content used in different context include removal of the iconic “Vietnam napalm girl” and censoring of the human rights abuses of the Rohingya
could be therefore covered by the same injunction, regardless of the context in which they are used. This very case note might be deleted from Facebook as it mentions that Eva Glawischnig-Piesczek was insulted as a corrupt oaf and traitor to her people.

As mentioned in section 5.1.4 above, there is a significant risk of over-removal or over-blocking when the filtering is done through automated search tools and technologies. Correct identification of content through automated tools remains challenging for content used in a different context, e.g. as a parody or quotation.\footnote{106} As acknowledged in the Impact Assessment to the DSM Directive, automated filtering tools easily provide “false positives” by incorrectly identifying content as unlawful, which leads to removals of legitimate content.\footnote{107} Even tools that rely on Artificial Intelligence are unable to understand irony or satire or realize that hate speech can be used in a quote to raise awareness.\footnote{108}

This means that applying the generally sensible rule that content identical or equivalent to what has been previously declared defamatory should also be removed or blocked might create problems from a fundamental rights perspective when it is implemented in practice. Requiring removal or blocking of any mention of such content, in whatever context, could hamper debate on important societal issues and negatively influence the exercise of freedom of expression and access to information. In the past, the ECJ has recognized this problem. It stated that a filtering system could “undermine freedom of information since that system might not distinguish adequately between lawful and unlawful content, with the result that its introduction could lead to the blocking of lawful communications”.\footnote{109}

5.2.3. Human review of automated decisions

To ensure that the interference with freedom of expression and information is proportionate, the injunction should be subject to a number of safeguards. One of these safeguards could be to have a “human in the loop”. This could mean that the removal of identical and equivalent content is not fully automated, but


109. Case C-70/10, Scarlet Extended, para 52; Case C-360/10, SABAM, para 50.
automated tools are only used to pre-select content and the final decision is taken by human content moderators. Intermediaries’ employees could also review and correct decisions made by automated filters in some sort of appeal process.

The DSM Directive and the proposed Terrorist Content Regulation provide for the review of automated filtering decisions by humans. Article 17(9) of the DSM Directive states that “decisions to disable access to or remove uploaded content shall be subject to human review”. The proposal for the Terrorist Content Regulation requires “effective and appropriate safeguards” against wrongful removal, including human evaluation of filters’ decisions (Art. 9). In the Parliament draft, human review is mandatory for platforms using filters, whereas in the Commission and Council drafts it is required only “where appropriate and, in any event, where a detailed assessment of the relevant context is required”. Both instruments introduce human assessment in the content moderation process to mitigate the risks of over-compliance by mistake-prone filters and prevent disproportionate interference with fundamental rights. This approach follows recommendations by human rights organizations, including the Council of Europe, which stated that “[d]ue to the current limited ability of automated means to assess context,” platforms that use filters should “ensure human review where appropriate”.

In contrast, the ECJ seems to exclude human review in Glawischnig-Piesczek when it implies that intermediaries should be able to comply with the injunction with the help of automated search tools and technologies. Platforms are still free to employ human review, but national courts are prevented from requiring human review because of the ECJ’s interpretation of Article 15(1) of the eCommerce Directive. This is problematic from a fundamental rights perspective. Human review of automated decisions certainly does not guarantee that content that is protected by freedom of expression and information remains on the digital platform.


111. Committee of Ministers, Recommendation CM/Rec(2018)2 to Member States on the roles and responsibilities of internet intermediaries, Adopted on 7 March 2018 at the 1309th meeting of the Ministers’ Deputies.


However, it is hard to imagine how proportionality of automated content moderation can be ensured without any human review. In any event, human review must be possible as part as an appeal process, as any objections to the removal of online content would require human review of the initial decision taken by the filters. Mistakes resulting from inaccurate assessments of online content may happen, but in such cases a path for a relief – through a correction of the initial decision – should be available. This is also important to uphold the right to an effective remedy.

5.3. Worldwide removal

In the final part of the judgment, the ECJ found that the eCommerce Directive did not preclude injunctions to remove identical and equivalent content from producing worldwide effects. In the view of the Court, the eCommerce Directive did not at all determine the territorial scope of domestic injunctions. It simply did not regulate this matter. Hence, it fell entirely within the discretion of the Member States to decide whether injunctions to remove identical and equivalent content could have worldwide effect. As the Court had already indicated when interpreting Article 18 of the Directive, the Member States had a “particularly broad discretion” when adopting measures intended to terminate and prevent infringements related to the activities of information society services.

However, the ECJ mentioned that the Member States had to take into account the “rules applicable at international level” when adopting these measures. According to the Court, this was apparent from Recitals 58 and 60 of the eCommerce Directive. It is not entirely clear what the phrase “rules applicable at international level” or “règles applicables au niveau international” – in the French version of the judgment – means. According to Recital 58, the eCommerce Directive is “without prejudice to discussions within international organizations (amongst others WTO, OECD, UNCITRAL) on legal issues”. This could imply that the ECJ referred to international treaty law in a broad sense. In this vein, the rules applicable at


Law and Information Technology, 91–121, at 108.

114. Keller, op. cit. supra note 84.
116. Ibid., para 49.
117. Ibid., paras. 50, 29 and 30.
118. Ibid., paras. 51–52.
international level seem to include international and regional human rights conventions.\textsuperscript{119}

Regarding the territorial scope of domestic measures obliging intermediaries, the ECJ adopted a different approach in \textit{Glawischnig-Piesczek} and in \textit{Google}, which was delivered a week earlier.\textsuperscript{120} In \textit{Google}, the ECJ did not refrain from ruling on the territorial scope of the right to be forgotten under EU data protection law. It found that where a search engine operator removes a web page from the list of results to comply with the right to data erasure, that operator is not required to de-reference the web page on all versions of its search engine worldwide. The difference between the two cases seems to be related to the different degree of harmonization of the relevant national measures by EU law. The EU legislature has harmonized the relevant material rules on data protection, but it has not harmonized the material rules on harm to personality rights, including defamation.\textsuperscript{121} The injunction at issue in \textit{Glawischnig-Piesczek} was determined merely by the eCommerce Directive, which leaves broad discretion to the Member States. Moreover, unlike the eCommerce Directive, the Data Protection Directive did address jurisdictional aspects of its application, basing its approach mainly on the territoriality principle of international law.\textsuperscript{122}

It is true that the eCommerce Directive does not address explicitly the territorial scope of national injunctions that are adopted pursuant to its Article 18. Nevertheless, it is regrettable that the ECJ shied away from answering the third question asked by the Austrian Supreme Court. The cross-border nature of the internet raises difficult questions from a jurisdictional perspective and national courts would surely be grateful for any guidance by the ECJ.

If the ECJ had ruled on the territorial scope, it would have needed to consider the repercussions that an injunction with worldwide effect might have on freedom of expression and information. Worldwide removal or delisting orders may have detrimental effects on freedom of information and expression. Other States, including authoritarian States, could follow the example of the EU and give worldwide effect to their removal orders.\textsuperscript{123} In \textit{Google}, Advocate General Szpunar saw “a genuine risk of a race to the

\textsuperscript{119} Spindler, op. cit. supra note 72, at 3276.

\textsuperscript{120} Case C-507/17, Google LLC, successor in law to Google Inc. v. Commission nationale de l’informatique et des libertés (CNIL), EU:C:2019:772.

\textsuperscript{121} Opinion, paras. 78–79. See also de Gergorio, “Google v. CNIL and Glawischng-Piesczek v. Facebook: Content and data in the algorithmic society”, (2020) Media Laws.


\textsuperscript{123} De Gergorio, op. cit. supra note 121.
bottom, to the detriment of freedom of expression” if the signal is sent to third
countries that they could order worldwide de-referencing of websites in
search results under their own laws. For this very reason, the ECJ should
have applied the Google approach by analogy and excluded the worldwide
effect of national injunctions aimed at obliging intermediaries to remove
illegal online content.

It will now be for the national court to determine the territorial scope of the
injunctions at issue in this case. The Austrian Supreme Court will have to
assess whether Austrian courts are competent to issue an injunction that has
effects outside of Austria. EU secondary law on jurisdiction and the
recognition and enforcement of judgments in civil and commercial matters
and the relevant case law of the ECJ can guide this analysis to some extent.

6. Conclusion

Glawischnig-Piesczek has triggered rather diverging reactions so far.
Facebook, several digital rights NGOs, and many commentators have
expressed concern about the implication of the judgment for freedom of
expression. On the other hand, commentators in Austria and Germany have
mainly emphasized that the judgment strengthens the protection of victims of
online hate speech and defamation, or noted that the judgment is in line
with their national case law on the extent of injunctions.

Commission nationale de l’informatique et des libertés (CNIL), EU:C:2019:15, para 61.
125. Klicka, “Der örtliche Wirkungsbereich gerichtlicher Löschungsanordnungen im
Lichte der E des EuGH C-18/18 Glawischnig-Piesczek/Facebook Ireland”, (2019) Medien und
126. Ibid.
127. Satariano, “Facebook can be forced to delete content worldwide, E.U.’s top court
facebook-europe.html>; Pichler and Riegler, “Gemischte Reaktionen auf weltweite
Löschpflicht für Hasspostings auf Facebook” (3 Oct. 2019), Der Standard, <www.derstand
ard.at/story/2000109402279/eugh-facebook-muss-hasspostings-weltweit-loeschen>;
European Digital Rights, “CJEU ruling on fighting defamation online could open the door for
upload filters” (3 Oct. 2019), <edri.org/cjeu-ruling-could-open-the-door-for-upload-filters/>;
Keller, op. cit. supra note 49.
(2019) Österreichische Juristen Zeitung, 893–907, at 893; Pichler and Riegler, op. cit. supra
note 127.
für Verbraucherrecht, 229–231, at 231; Spindler, op. cit. supra note 72, at 3275.
It is clear that the ECJ has taken a new approach to Article 15(1) of the eCommerce Directive in the present case. In the past, the ECJ excluded obligations that required intermediaries to observe all the data of all the users of their platform. In *Glawischnig-Piesczek*, the Court ignored this rigid criterion and opted instead for a more flexible interpretation of Article 15(1). It concluded that national courts may issue an injunction that requires an intermediary to remove or block online content that is identical or equivalent to content that has previously been held to be illegal by a court, irrespective of who generated this content. It did not matter that the intermediary would have to search through all the uploads on its platform to identify identical or equivalent content. What previously has been seen as general monitoring, could now, under certain conditions, be qualified as specific monitoring, and therefore allowed by the eCommerce Directive. Unfortunately, the ECJ did not distinguish its new approach from its previous one.

The ECJ should be praised for ensuring the effective protection of individuals from online defamation. The Court was right to observe that the eCommerce Directive recognized the importance of effective national injunctions that are aimed at ending unlawful online activities. Moreover, it is to be welcomed that the Court considered the actual realities of the dissemination of content on social media platforms in its analysis. It would indeed be easy to circumvent an injunction that is restricted to identical content or to content by the same user. The judgment undoubtedly attempts to address the problem of practical implementation and effectiveness of injunctions for illegal online content.

The judgment in *Glawischnig-Piesczek* is in line with a more general trend in EU law, namely the trend to impose more responsibilities and more obligations on intermediaries in order to offer better protection from illegal online content. The monitoring obligations introduced by the new DSM Directive and proposed in the Terrorist Content Regulation signal that policymakers are increasingly concerned about the amount of illegal online content and its impact on the rights of individuals.

By adopting a new approach to Article 15(1) of the eCommerce Directive in *Glawischnig-Piesczek*, the ECJ might also have laid the ground for a more flexible interpretation of this provision in future cases. This could help to resolve the inherent conflict between the new monitoring obligations that are imposed on intermediaries through specific legislation such as the DSM Directive and the prohibition of general monitoring obligations, which remains valid.

At the same time, it is important not to overstate the implications of *Glawischnig-Piesczek*. The understanding of general monitoring that the Court adopted in this case is restricted to the specific context of injunctions...
adopted by national courts. What is understood as general monitoring in another context is still open for debate. There is a serious concern, however, that Glawischnig-Piesczek marks the start of a new trend that will lead to considering all kinds of monitoring as specific, making the prohibition of Article 15(1) of the eCommerce Directive effectively meaningless.

Regarding injunctions, the Glawischnig-Piesczek judgment only addressed some of the issues that are relevant from the perspective of a national court. A number of important issues were left open. For instance, the ECJ did not explain how a national court should specify content that is equivalent to content that has previously been held to be illegal. Should it draw up a list of equivalent content or spell out what it is that made the original content illegal? It can be expected that there will be disputes about the classification of content as equivalent.

Moreover, the balancing exercise conducted by the Court only took into account the rights and interests of the defamed individual and of the intermediary. The judgment failed to consider the overall effect of the injunction on the fundamental rights of other users, in particular of their freedom to expression and information under the Charter of Fundamental Rights. The Court did not give the national court any guidance on how this right should be balanced against competing interests. This is regrettable since it is the role of the ECJ to interpret EU secondary law in light of the Charter. The ECJ also shied away from ruling on the territorial scope of national injunctions. Thus, a number of difficult tasks were left to the Austrian Supreme Court, which had not delivered its final judgment when this case note was submitted.

This lack of guidance from the ECJ is problematic. National courts are increasingly faced with challenging legal questions regarding the responsibilities of intermediaries for user-generated content. The ECJ should help them by giving comprehensive answers to any questions they might have on the interpretation of Section 4 of Chapter II of the eCommerce Directive. More comprehensive answers would also lead to some convergence of the various national approaches, which is beneficial due to the inherently cross-border nature of the internet. National courts will need guidance from the ECJ on how to interpret the eCommerce Directive in the light of new challenges faced online as long as the EU legislature has not come up with a new regime for intermediary responsibility in the new Digital Services Act.

Finally, another problematic aspect of the judgment concerns the ECJ’s assumptions regarding automated filtering tools. In particular, the assessment that access to automated search tools and technologies provides a non-problematic solution to the problem of finding illegal content online
seems to be based on a misconstrued understanding of how filtering works in practice. The Court’s exclusion of human review of automated filtering decisions also goes against the recent trend that uses “human-in-the-loop” review as a safeguard against erroneous decisions.

Clara Rauchegger and Aleksandra Kuczerawy*

* Assistant Professor, University of Innsbruck and Postdoctoral Researcher, KU Leuven, respectively. The authors are grateful to the anonymous reviewers for their helpful comments.