Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations (C18/18 Glawischnig-Piesczek v Facebook Ireland)

Glawischnig-Piesczek v Facebook on the expanding scope of Internet Service Providers' Monitoring Obligations

Paolo Cavaliere
Lecturer at the University of Edinburgh Law School, UK. For correspondence: <paolo.cavaliere@ed.ac.uk>.

Case C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Limited, Judgement of the Court of Justice of the European Union (Third Chamber) of 3 October 2019

Article 15(1) of the E-Commerce Directive does not preclude a court of a Member State from: ordering a host provider to remove or block access to information identical to the content of information previously declared unlawful; ordering a host provider to remove or block access to information equivalent to information previously declared unlawful, provided that the content remains essentially unchanged and the differences in the wording are not such as to require the host provider to carry out an independent assessment beyond the elements specified in the injunction; ordering a host provider to remove or block access to information covered by the injunction worldwide within the framework of the relevant international law.

Recitals 6, 7, 9, 10, 40, 41, 45 to 48, 52, 58 and 60; Articles 14, 15(1) and 18(1) of Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L 178/1

I. Background

The case originates from a request by the former Austrian MP and spokeswoman of the Green Party to remove a post shared on her own private Facebook account by a user, consisting of a news article covering the refugee crisis in Austria and comments on the topic made by the plaintiff in an interview, alongside personal comments which, the European Court summarises, 'the referring court found to be harmful to the reputation of the applicant in the main proceedings, and which insulted and defamed her'.[1]

After a request to remove the user's post was declined by the platform, the plaintiff filed a petition to the Commercial Court of Vienna; the Court considered that Facebook, by failing to remove the original post on the plaintiff's first notice, was not covered by the exemption from secondary liability and ordered the platform to remove both the original post any further content that would include the plaintiff's picture alongside identical or analogous comments.[2]

On appeal, the Higher Regional Court of Vienna found that such an obligation would be tantamount to an obligation of general monitoring and thus incompatible with the E-commerce Directive; it thus removed the second part of the injunction, while upholding that the original post was manifestly unlawful and should have been removed by the platform following the first notification from the plaintiff. The Higher Court also confirmed that Facebook should remove any future posts that would include the same derogatory text

[1] Para. 12.
[2] Para. 14.

alongside any image of the plaintiff.[3] Facebook appealed this decision to the Austrian Supreme Court, which in turn referred to the CJEU two main ranges of questions:[4]

- First, whether ordering a host provider to remove posts that are identically worded to other illegal content is compatible with Article 15(1) of the E-Commerce Directive. In case of a positive answer, the referring court asked whether this obligation could expand beyond identical content and include content that is analogous in substance, despite a different wording. These were ultimately questions concerning the responsibility that platforms can be given in making their own assessment of what content amounts to unlawful speech, and what are the limits of active monitoring.

- Second, whether national courts can order platforms to remove content only within the national boundaries, or beyond ('worldwide'). This was a question concerning the admissibility of extra-territorial injunctions for content removal.

II. Decision of the Court

The Court has answered all the questions in the affirmative, qualifying as specific monitoring obligations compatible with the E-Commerce Directive injunctions to remove or block access to information identical or equivalent to the content of information previously declared unlawful.

The Court considered that Facebook did not meet either of the two conditions to be exempted from liability provided for by Art 14(1) of the E-Commerce Directive, as it both had knowledge of the illegal information and failed to remove it expeditiously.[5] Against this background, it then went on to discuss the limits of obligations that can state authorities can impose to intermediaries in such circumstances.

A starting point in this analysis is that, pursuant to Art 18 of the E-Commerce Directive, national courts can adopt measures to terminate infringements, and in so doing have a 'particularly broad discretion' with regard to the kind of actions, procedures and scope of the injunctions imposed.[6] However, an explicit limit is provided by Art 15, which prohibits Member States to impose general monitoring obligations, or general obligations to actively seek facts or circumstances that indicate illegal activities (general monitoring obligations), on intermediaries carrying out activities such as those described in Art 12-13-14 (i.e. acting as mere conduits, caching or hosting information). By contrast, Recital 47 allows to impose monitoring obligations 'in a specific case'.[7] The remitting court asked the CJEU to determine whether the injunctions imposed on Facebook belong to any of these categories.

With regard to the first question, the CJEU finds that an order 'to remove or block access to information which [a host provider] stores, the content of which is identical to the content of information which was previously declared to be illegal'[8] cannot be regarded as either a general monitoring obligation or an active general monitoring obligation.[9]

The CJEU then moves on to consider whether an order 'to remove information which [a host provider] stores, the content of which is equivalent to the content of information which was previously declared to be illegal'[10] is compatible with the Directive. Moving from the consideration that the illegality of the content depends substantively on the content conveyed,

---

[3] Para. 16.
[4] Para. 20.
[5] Para. 27.
[6] Paras. 29-30.
[7] Para. 34.
[8] Para. 33.
[9] Para. 37.
[10] Para. 38.

rather than on the combination of words used,[11] and for an injunction to achieve its objectives effectively it needs to extend to information the conveys 'essentially' the same message as the other content previously declared illegal.[12] As a result, an injunction ordering the removal of – or to block access to – such 'equivalent' content is compatible with the E-Commerce Directive, provided that includes 'specific elements … such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined'[13] as to allow a host provider to identify such information without the need to carry out 'an independent assessment of that content'.[14]

Finally, the Court observes that the E-Commerce Directive 'does not make provision … for any … territorial limitation'[15] regarding the scope of monitoring obligation: as a result, such obligations can be imposed worldwide within the framework of the relevant international law.

III. Commentary

This decision, long awaited and yearned for its possible impact on the shape of on-line speech in the near future, leaves a bittersweet taste. While in principle some of its findings may seem reasonable, looming questions regarding both the practicalities of monitoring obligations imposed on service providers' obligations and the compatibility of extraterritorial injunctions with international law remain open. It may be that it will take some painfully wrong attempts before domestic and international decision-makers strike the right balance.

1. The Limits of Monitoring Obligations

With regard to the issue of the reappearance of identical content, the Court taps onto an increasingly pressing problem of on-line speech and it is certainly right to consider that a 'genuine risk'[16] of illegal content being reproduced and shared again by other users exists and needs to be addressed in a timely and effective fashion. However, the conclusion that obligations to remove content identical to other information already found illegal would be compatible with the limitations imposed by the E-Commerce Directive seems to be accepted as self-explanatory with little to no guidance. In particular, the Court does not elaborate explicitly on the reason why an obligation to seek and remove identical content would not constitute an active monitoring obligation. The Advocate General in his opinion had elaborated on this question much more at length: a central element in his reasoning was that 'the reproduction of the same content by any user of a social network platform seems, … as a general rule, to be 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'.[17] The Court evidently followed this line of reasoning, and all too quickly has jumped to the conclusion that that host providers could rely, in discharging the duties imposed on them, on 'automated search tools and technologies'.[18]

---

[11] Para 40.
[12] Para. 41.
[13] Para. 45.
[14] Ibid.
[15] Para. 49.
[16] Para. 36.
[17] Opinion of AG Szpunar, para. 61.
[18] Para. 46.

More detail is provided instead on the question regarding the removal of content that is equivalent to information previously declared illegal. Devising a two-part test of a sort, the Court concluded that, in order to determine the equivalence of different items of information, consideration needs to be given both to the substantive information conveyed and whether it amounts to 'essentially … the same message'[19] as the original post, and to the wording, which may in turn be 'slightly different'.[20] The part of the test that focuses on the wording is seemingly more relaxed as it leaves room for lexical variations, yet it requires that any '[d]ifferences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content'[21] taking avail of the guidance provided by 'specific elements'[22] laid out in the injunction.

Despite the centrality of the notion of independent assessment to determine what monitoring obligations are compatible with the E-Commerce Directive, the Court provides little practical guidance on it. Both the AG and the Court envisaged that recourse to technology would exempt host providers from making independent assessments; however, relying on the ability of technology to perform such a task is, at present, a gamble to say the least. As noted in relevant literature, whereas 'human cognition relies upon attention to collateral information that exists beyond any specific situation that may be at hand at any given time ... the very trait that [AI technology] cannot yet exhibit is the ability to leverage vast amounts of unrelated data from inductive experience that can alter the desired (or expected) outcome of a situation. In short, AI does not yet understand the context within which it is operating'.[23] Given the current state of available technology, the assumption that intermediaries would be exonerated from making independent assessments by taking avail of AI seems misplaced. Platforms will still need to resort to human curation to make a number of substantive assessments, including the context in which information is reproduced, either in an identical or equivalent form (discerning if it is meant to satirise or criticise the original content, for instance). It is also remarkable that, contrary to the suggestion of the AG,[24] the Court makes no reference to a requirement that monitoring obligations are limited in time: as a result, platforms could face open-ended obligations to continue assessing the ongoing relevance of any circumstances that had contributed to determine the illegality of the original information (for the sake of argument: would a decision like the one in comment effectively shield politicians, who had successfully filed a suit against a post on social media, from any similar future criticism irrespectively of any new statements or actions they could have subsequently made? What would happen if the defendant in a libel suit had failed to establish the defence of truth, but new revelations subsequently emerged?).

As things stand, the decision marks another step in the direction of expanding the limits of active monitoring that intermediaries are expected to perform: a trend happening at the global level[25] with worrisome consequences for the freedom to impart and receive information.

---

[19] Para. 41.
[20] Ibid.
[21] Para. 45.
[22] Ibid.
[23] Sean Kanuck, 'Humor, Ethics, and Dignity: Being Human in the Age of Artificial Intelligence' 33 (2019) Ethics & International Affairs 3, 7.
[24] Opinion of AG Szpunar, para. 49.
[25] See generally Giancarlo F Frosio, 'The Death of "No Monitoring Obligations": A Story of Untameable Monsters' 8 (2017) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 199.

In lack of available technological solutions, we are left at present with the notion that the scope of specific monitoring obligations compatible with the E-Commerce Directive goes beyond merely technically cross-checking the similarity of language and includes more substantive assessments such as the discretionary contextualisation of information, and can be expected to be imposed with no restrictions in time and space, as discussed in the next section.

2. The Scope of Extraterritorial Injunctions

The second notable profile in this decision concerns the geographical scope of injunctions to remove or take down content, something that with no doubt is going to ignite more discussions in the future. The detrimental effect for freedom of expression and the right to receive information seems obvious, as this opens the door for any State to impose its own standards of acceptable speech across its domestic boundaries, and effectively limit the accessibility of information to Internet users based in countries where such information may well be lawful. It is all the more baffling, in a sense, that this decision originates from a defamation suit, and follows on a long-standing question on the issue of 'libel tourism'. This decision is likely to complicate things even further.

On the basis of the Recast Brussels Regulation[26] and a stream of CJEU decisions (most relevantly *Bier*,[27] *Shevill*[28] and *eDate*[29]), plaintiffs enjoy a wide discretion in selecting the forum where they intend to bring an action, whether it is the courts of the place where the damage had occurred (c.d. *locus damni*, which in the context of on-line publications, it is anywhere the content was accessible), of the place where the event that caused the damage happened (c.d. *locus acti*, which in the context of libel suits is the place where the publisher is established and practically coincides with the forum defendant rule), or of the place where the plaintiff has their main centre of interest (c.d. *forum actoris*). However, following *Bolagsupplysningen*[30] only the courts of either the *locus acti* or the *forum actoris* have jurisdiction for the entirety of the harm and can issue injunctions for the correction or removal of content. It is interesting to note that while the Court in *Bolagsupplysningen* departed from the AG's opinion, which had instead suggested that all competent courts, included those of the *locus damni*, should be able to order the removal of information, the Court and the AG had reached different conclusions both moving from the same premise, a supposed 'universal'[31] or 'unitary nature'[32] of Internet content.[33] The decision in *Glawischnig* evidently builds on the same understanding and reinforces this idea, providing an explicit underpinning for those courts with jurisdiction over the entirety of the harm to grant injunctions to remove content worldwide. Two orders of considerations follow from this: the first regarding the issue of prescriptive and enforcement jurisdiction in defamation claims, and the second regarding the recourse to technological means.

---

[26] 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 351/1.
[27] Case C-21/76 Handelskwekerij Bier v Mines de Potasse d'Alsace [1976] ECLI:EU:C:1976:166.
[28] Case C-68/93 Shevill and Others v Presse Alliance [1995] ECLI:EU:C:1995:61.
[29] Case C-509/09 eDate Advertising and Others [2011] ECLI:EU:C:2011:685.
[30] Case C-194/16 Bolagsupplysningen and Ilsjan [2017] ECLI:EU:C:2017:766.
[31] *Bolagsupplysningen* (n 17) para. 48.
[32] Opinion of AG Bobek, para. 126.
[33] For a (critical) comment on this specific stance in *Bolagsupplysningen* see Cedric Vanleenhove, 'The European Court of Justice in Bolagsupplysningen: The Brussels I Recast Regulation's jurisdictional rules for online infringement of personality rights further clarified' 34 (2018) Computer Law & Security Review 640, 645.

2.1 Prescriptive and enforcement jurisdiction in defamation claims

Firstly, the issue of extra-territorial injunctions needs to be considered against the background of the exclusion of defamation and privacy from the Rome II Regulation,[34] which in turn makes defamation suits subject to the existing choice of law rules in the Member States. In the case at stake, the Court did not have the opportunity to consider in depth all the possible ramifications of on-line defamation and choice of law as this was indisputably a case governed by Austrian law. However, future scenarios may well be less straightforward and add further layers of intricacy. If the exclusion of defamation and privacy torts from the scope of EU harmonisation contributed to preserving the capacity of each forum's legal order to strike its own balance between free speech and competing rights,[35] then the *Glawischnig* decision evidently defies this purpose.

However, it is possible that the effective impact of this decision will be less substantial than it may appear to be. The CJEU in fact has affirmed that while the E-Commerce Directive does not preclude extraterritorial injunctions, it is only possible to grant extraterritorial injunctions 'within the framework of the relevant international law'.[36] Whether any State can claim prescriptive jurisdiction in matters of libel law is, and still remains after this decision, a disputed question under international law. The possibility to exercise domestic jurisdiction over foreign publishers for defamation claims stands on the shaky grounds of a few highly controversial decisions, such as Australia's *Gutnick*,[37] Ontario's *Bangoura*[38] (where, notably, the Court of Appeal found that States should avoid claiming extraterritorial jurisdiction when a publisher had implemented measures to restrict the availability of that content locally: this point will be discussed further below) and a few from English courts prior to the Defamation Act 2013.[39]

In reaction to such attempts to subject foreign publishers to domestic defamation laws, refusals to enforce foreign defamation judgements are a common response from States concerned about protecting their own local standards of freedom of expression. This is well exemplified by the case of the USA, where both influential decisions such as *Bachchan*[40] and the more recent SPEECH Act[41] expressly require courts not to recognise foreign defamation judgements if either the publication would be protected by the First Amendment, or the foreign court lacks personal jurisdiction under the Due Process Clause.[42] The *Glawischnig* decision at its face value would effectively force legal orders to bear the consequences of decisions made in different States pursuant to their own systems of values and principles, simply as a

[34] Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L 199.
[35] Alex Mills, 'The law applicable to cross-border defamation on social media: whose law governs free speech in "Facebookistan"?' 7 (2015) Journal of Media Law 1, 13-14.
[36] Paras. 51-53.
[37] Gutnick v Dow Jones & Co Inc [2002] HCA 56; (2002) 77 ALJR 255.
[38] Bangoura v Washington Post & Others [2005] O.J. NO. 3849.
[39] See generally Aaron Warshaw, 'Uncertainty from Abroad: Rome II and the Choice of Law for Defamation Claims' (2006) 32 Brook. J. Int'l L. (2006) 269, 283-289.
[40] Bachchan v. India Abroad Publications Inc., 585 N.Y.S.2d 661 (Sup. Ct. 1992).
[41] Securing the Protection of Our Enduring and Established Constitutional Heritage Act, 28 U.S.C. § 4102 (2011).
[42] See generally Darren J Robinson, 'U.S. Enforcement of Foreign Judgments, Libel Tourism, and the SPEECH Act: Protecting Speech or Discouraging Foreign Legal Cooperation' (2013) 21 Transnat'l L & Contemp Probs 911.

consequence of the material disappearance of information bypassing the issue of foreign enforcement. The lack of international consensus on the legitimate exercise of extraterritorial jurisdiction for defamation claims and the reluctance of certain States to accept jurisdictional claims from other States to the point of adopting dedicated blocking statutes, both motivated by different substantive standards of freedom of expression and protection of reputation across different legal systems, strongly suggest that international law hardly provides a robust basis for domestic courts to grant worldwide blocking or removal injunctions,

2.2 Worldwide enforcement and geo-blocking

Secondly, the decision reveals a struggle to grapple with technology and the opportunities it opens. Until recently, when libelous publications happened to be mostly in physical print, remedies were simply and plainly restricted in their territorial scope by the limited capacity of courts to enforce their decisions beyond national boundaries.[43] With the emergence of the Internet and the reality of information becoming available across States, the issue was once again largely left to contingent circumstances (for instance, website operators would often voluntarily withdraw content in response to foreign decisions, in an attempt to prevent future litigation[44]) more than legal considerations. This decision comes at a momentous time for technological development as the reality of geo-location technologies frustrates the assumption of a borderless Internet. Since targeting users depending on their locations has become the norm for Internet services, it has been observed that courts could well adopt the default approach of expecting service providers to exclude (or 'dis-target') users located in those areas where they are not prepared to accept liability.[45]

The failure to take into account the easy possibility of resorting to geo-locating technologies is particularly relevant in light of a further element in this decision. The European Convention of Human Rights requires any restrictions to speech to pass a test of necessity and proportionality, including the geographical scope of limitations[46] which ought to be construed as narrowly as possible. As a matter of fact, it remains dubious whether under the ECHR framework a worldwide removal of Facebook posts would qualify as the least restrictive measure to protect the reputation of a politician who, at the time of the dispute, had only held offices at the national level.

On a more fundamental level, there is some bitter irony in the fact that the Court on the one hand envisaged technology as offering an escape route where there is really none at present, and mistakenly decided to rely on AI to assess the substantive equivalence of different items of information; and on the other hand it missed an opportunity to entrust a widely available technology to resort to a more narrowly construed limitation to speech. Quite evidently, this is a failure to take avail of technological development to strengthen the legal framework of online speech and provide an adequate territorial scope to the protection of personality rights. Hopefully the Court will soon have the opportunity to correct the mistake in a future decision informed by a stronger understanding of technology and its implications.

---

[43] Trevor C Hartley, '"Libel Tourism" and Conflict of Laws' 59 (2010) International and Comparative Law Quarterly 25, 27.
[44] Mills (n 37) 19.
[45] Dan JB Svantesson, 'Time for the Law to Take Internet Geolocation Technologies Seriously' 8 (2012) Journal of Private International Law 473.
[46] Cf. *Christians Against Fascism and Racism v United Kingdom* App no 8440/78 (ECtHR, 16 July 1980).