

ANNOTATIE

Eva Glawischnig-Piesczek (HvJ EU, zaak C-18/18) - CJEU clarifies hosting providers' obligations to remove defamatory content, for now

T. McGonagle

Annotatie bij Hof van Justitie van de Europese Unie, 03-10-2019, ECLI:EU:C:2019:821 (EHRC-2020-0042)

1. In the *Eva Glawischnig-Piesczek* case, the Court of Justice of the European Union (hereafter, CJEU) grappled with several thorny questions of internet intermediary liability and jurisdiction, including the extra-territorial impact of defamatory content. These are thorny questions because defamatory content can be reproduced or re-purposed, shared and spread online, in particular via social media, with great speed, reach and impact. This means that viral content can cause lasting damage to a person's reputation with great alacrity. A further complication is that defamation laws across the globe vary significantly in nature. When national court injunctions aim to have extra-territorial effects, differences between defamation laws can become problematic.

2. At the operative time, the applicant, Eva Glawischnig-Piesczek, held a number of positions within the Austrian political party, The Greens. In April 2016, a Facebook user shared on that user's personal page an article from an Austrian online news magazine. This created a thumbnail of the original article, containing the title of the article, a short summary and a photo of the applicant. The user also published – in connection with the article – a comment which the Austrian courts held to have been harmful to the applicant's reputation and to have insulted and defamed her. The post was accessible for any Facebook user.

3. The applicant asked Facebook Ireland (the operator of Facebook's services outside of the US and Canada) to delete the comment. When Facebook Ireland refused to do so, the applicant initiated legal proceedings before the Austrian courts. An interim injunction by the Commercial Court, Vienna, directed Facebook Ireland to cease and desist from publishing and/or disseminating the comment or content with equivalent meaning. Facebook Ireland then disabled access in Austria to the original content. The Higher Regional Court in Vienna, on appeal, distinguished between the identical allegations (upholding the lower court's order) and equivalent content (the dissemination of which only had to cease in respect of such content that was brought to the knowledge of Facebook Ireland). Both parties appealed to the Austrian Supreme Court on points of law, which requested a preliminary ruling on a few questions from the CJEU.

4. The questions concerned the interpretation of the Electronic Commerce (hereafter E-Commerce) Directive, namely whether Article 15(1) of the Directive generally precludes an obligation on host providers to expeditiously remove from its services, once it has knowledge of it, illegal information and information with equivalent meaning, in the relevant Member State and worldwide.

5. The main aim of the E-Commerce Directive is to seek "to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States".¹ The Directive is premised on a contemporary understanding of how internet intermediaries worked in 2000 when the Directive was adopted, namely that intermediaries either have a passive or an active relationship with third-party content disseminated through their networks or services. In the logic of this binary distinction, the drafters of the Directive sought to ensure that passive intermediaries would not be held liable for content over which they had no knowledge or control. The Directive thus establishes a "safe harbour" regime for passive intermediaries.

6. The "safe harbour" regime entails exemptions from liability in "cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored".² These exemptions are set out in Articles 12-14 of the Directive and they can be availed of by service providers acting as a 'mere conduit' for information, or those which provide 'caching' or 'hosting' services. This means that

intermediaries which serve as hosting providers – like Facebook in the present case - would ordinarily benefit from an exemption for liability for illegal content, as long as they maintain a neutral or passive stance towards that content. A service provider that hosts third-party content may avail of this exemption on condition that it does not have “actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent” and that “upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information”.³ However, “the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level”.⁴

7. Under Article 15(1) of the Directive, EU Member States are not allowed to impose a general obligation on service providers to “monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity”. Such a general monitoring or searching obligation would entail surveillance activities that would have a chilling effect on the freedom of expression of users of the service. This prohibition only concerns obligations of a general nature; it does not apply to “monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation” (Recital 47).

8. The present case concerns a particular piece of defamatory information, as identified by the Austrian courts. The CJEU held that this was specific enough not to fall foul of Article 15(1). But that is not the end of the matter. Social media facilitate and even incentivize the sharing, spreading and re-shaping of content. Consequently, if a court order were to be directed only at a specific piece of information, variants of that information could be created and disseminated which would for all intents and purposes have the same harmful impact as the original, specific piece of information. It was in anticipation of such a legal loophole that the Austrian Supreme Court sought interpretative guidance from the CJEU on the words “information with an equivalent meaning”.

9. The CJEU appreciated this concern and stated that “in order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, in addition to any further impairment of the interests involved, to be capable of achieving those objectives effectively, that injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal” (para. 41). It also went along with the Austrian Supreme Court’s suggestion that “the

effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal, which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he is a victim” (*ibid.*).

10. Be that as it may, “equivalent” is a slippery term. Unless it is clearly and tightly defined, there is a risk that it will be interpreted overbroadly, with a potential chilling effect for free expression. To trammel the scope of the term, the CJEU underlined that the equivalent information at issue in the present case “contains specific elements which are properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal” (para. 45). It further cautioned that “Differences 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.” (*ibid.*).

11. The CJEU was satisfied that the extension of the obligation to “information with equivalent content” in the present case strikes an appropriate balance between the interests at stake. The CJEU found that it “appears to be sufficiently effective” for protecting the reputation of the person concerned and it stops short of imposing “an excessive obligation” on the host provider by requiring a general monitoring of content or an independent assessment by the host provider of the defamatory content of an equivalent nature (para. 46). The CJEU envisaged that “automated search tools and technologies” can be deployed by the host provider for those purposes (*ibid.*).

12. The final question for the CJEU to address concerned the implications of Article 18(1) of the Directive, which reads: “Member States shall ensure that court actions available under national law concerning information society services’ activities 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”. The CJEU found that this article does not provide for any limitation – territorial or otherwise – on the scope of the measures which Member States are entitled to adopt in this connection (para. 49). Accordingly, it does not preclude that injunctions issued by national courts could produce effects worldwide. However, relevant EU rules do have to be consistent with the rules applicable at the international level and Member States should ensure that any measures that they adopt which have worldwide effects “take due account of those rules” (para. 52).

13. This judgment has clarified that Article 15(1) of the E-Commerce Directive does not preclude a court of a Member State from ordering a host provider to remove information which it stores, the content of which is identical or equivalent to the content of information previously held to be unlawful, or to block access to that information, as long as such a requirement does not lead to monitoring or search obligations beyond the specific information in question (see para. 10, above) or an obligation to carry out an independent assessment of that content. Although this clarification is the *conclusion* of a particular judgment, it is sure to also be the *beginning* of a longer journey of discussion and interpretation. We can expect creative lawyers and scholars to eagerly exploit the inherent semantic chameleonism of the term, “equivalent content”.

Tarlach McGonagle

Leiden Law School and Institute for Information Law (IViR), Amsterdam Law School

Voetnoten

1 Article 1, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2000] OJ L 178/1 (Directive on Electronic Commerce).

2 Recital 42, *ibid.*

3 Article 14, *ibid.* See also L’Oréal and Others, CJEU (GC) 12 July 2011, Case C-324/09, ECLI:EU:C:2011:474.

4 Recital 46, *ibid.*