Escaping the Slippery Slope: Freedom of Expression and Cyberspace Regulation after the Delfi Case

Konstantina Georgaki, Emmanuel Giakoumakis, and Alessandro Rollo
Master of Law Programme, Faculty of Law, University of Cambridge

On 16 June 2015, the Grand Chamber of the European Court of Human Rights delivered the final judgment in *Delfi AS. v Estonia,* where it ruled that the decision to hold an Internet Service Provider liable for online, anonymous defamatory comments was compatible with the European Convention on Human Rights, thus raising serious concerns on the enjoyment of the right to freedom of expression on the Internet[1].

Delfi is one of the largest web news portals in Estonia. It allows users to post comments on news stories without requiring prior registration, which appear automatically without moderation, though the website has an automatic filter that deletes comments containing obscene words as well as a notice-and-take-down system that enables users to report defamatory comments. Defamatory comments are deleted by the company upon review. In January 2006, Delfi published an article on roads over the frozen sea in Estonia, which—although not defamatory in its nature—attracted a wide number of offensive comments. In March 2006, an individual known as L. requested Delfi to remove such defamatory comments and pay damages. As a result, Delfi removed immediately the comments. However, since it refused to pay damages, L. sued Delfi before an Estonian court, which issued a decision—later upheld by the Estonian Supreme Court—that awarded him damages in the amount of Euro 320. Delfi then challenged the judgment before the European Court of Human Rights, which rejected its application. The case was subsequently referred to the Grand Chamber of the Court.

Delfi claimed that the decision of the Estonian Supreme Court imposed an obligation to maintain a preventive censorship policy in violation of the right to freedom of expression provided for by Article 10 of the European Convention on Human Rights. This provision protects the 'freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.' However, the Convention allows restrictions on this right when they are 'prescribed by law and are necessary in a democratic society' to protect a number of legitimate aims, including national security, crime prevention, health, morals and the reputation or rights of others[2].

> If Internet Service Providers (ISPs) bore vicarious liability for illegal content uploaded by others, even if not aware of its existence, this would place a disproportionate financial burden on them

The most contentious issue of this case is not the limitation of the right to freedom of expression of anonymous commenters itself, but the decision to hold the news portal liable for the comments posted on its website by others. This type of liability is known as the vicarious responsibility of Internet Service Providers (ISPs). In the European Union (EU), the normative framework on ISPs' liability is laid down by the E-commerce Directive 2000/31/EC, which exempts hosting service providers (such as blogs or websites) from vicarious liability for the information stored at the request of a user (for example, a comment posted to a blog post). Under Article 15 of the

Directive, ISPs have neither an obligation to monitor the information they transmit or store, nor a general obligation to actively seek facts or circumstances indicating illegal activity. Their responsibility may only be engaged if the provider, upon obtaining knowledge of hosting illegal content, fails to act expeditiously to remove or disable access to the impugned information[3]. The underpinning idea is that if ISPs bore vicarious liability for illegal content uploaded by others, even if not aware of its existence, this would place a disproportionate financial burden on them to impose filtering systems, blocking measures and detection methods to prevent illegal content from being published online. However, once a user notifies the ISP of the illegal content, the latter is expected to act expeditiously to block the access thereto (notice-and-takedown procedure), otherwise it will bear responsibility for the subsequent legal consequences. This establishes a 'safe harbour' for ISPs, since they are immune from vicarious liability, as long as they have no knowledge of the illegality of the content that they host. In this vein, the European Court of Justice issued a judgment in 2012, declaring that ISPs do not have an obligation to filter content. The judgment precluded a national court from issuing an injunction against an ISP requiring it to install a system for filtering information stored on its servers by its users, at its own expenses, to identify and prevent the publication of content infringing copyright. This principle is applicable to all cases of illegal content, such as spyware, malware and also hate speech[4].

Nevertheless, the domestic courts of Estonia disregarded this framework and came up with a different reasoning, which was subsequently supported by the Grand Chamber. Contrary to Delfi's contention that the news portal should be classified as an ISP with regards to third-party comments, the Grand Chamber considered Delfi as the direct publisher of the content itself, thus placing vicarious liability for the illegal material on the intermediary. In a highly criticised line of reasoning, the Grand Chamber stressed that 'it is not its task to take the place of the domestic courts. It is primarily for the national authorities, notably the courts, to interpret and apply domestic law'[5]. Thus, it upheld the domestic courts' findings on the *legality* of the measure and explored whether this measure was the least burdensome and more proportionate in view of the legitimate aim pursued. Contrary to its previous case law that the punishment of a journalist assisting in the dissemination of statements made by others in the context of an interview would seriously hamper freedom of the press[6], the Grand Chamber held that it is legitimate to sanction the portal to protect another person's right. Although the comments in question had been removed upon notification by L., the person concerned, the Grand Chamber held that the portal exercised a substantial degree of control over the comments and, contrary to the Directive, should have prevented their publication in the first place. In view of the insignificant amount of the fine, the Grand Chamber held that the measure was proportionate and not in breach of freedom of speech.

The reasoning of the Grand Chamber is flawed in its foundations as it disregards the fact that imposing vicarious liability on ISPs may have a chilling effect on freedom of expression

The reasoning of the Grand Chamber is flawed in its foundations as it disregards the fact that imposing vicarious liability on ISPs may have a chilling effect on freedom of expression, in the sense that it will encourage ISPs to delete comments under the threat of sanction, thus leading to a 'slippery slope' that could shatter the architecture of the Internet as a whole. In the present case, the Grand Chamber addressed the issue of content regulation in cyberspace by striking a balance between safeguarding freedom of expression and providing a minimum level of protection to the other fundamental values involved. However, in its attempt to deliver a new interpretative approach to this end, the Grand Chamber did not properly weigh the potentially detrimental effects of its decision on freedom of expression in cyberspace. If ISPs are held vicariously accountable for the content that they

host, they will probably avoid the risk of incurring liability by imposing censorship on web users and limiting access proactively to their websites. This would not only hamper online freedom of expression, but could also entail catastrophic economic repercussions for e-commerce, as it would require ISPs to set up, at their own expenses, costly mechanisms of prevention and filtering systems for comments (which are highly profitable for marketing purposes), thus restraining the free flow of information on the Web.

Conclusion

In conclusion, in the *Delfi* case the Grand Chamber ignored the rationale underlying the current European regulatory framework. This further shows that such legal framework is not sufficient to preserve fundamental rights in cyberspace. The issue of cyberspace regulation, has now gained prominence and urgency once again, as *Delfi* made it clear that a new regulatory approach is imminently called for. Given the substantially de-territorialised features and transnational character of cyberspace, which pose significant difficulties to any national regulatory attempt, it can only be efficiently regulated on international or, at least, multinational level. Since international regulatory attempts have consistently been unsuccessful in the past and domestic approaches to the matter are confronted with considerable difficulties, the Internet had to develop mechanisms to effectively regulate itself (i.e. by implementing codes of conduct and mechanisms of self-correction, such as the notice-and-takedown procedure), so as to avoid the creation of a regulatory gap. The application of self-regulation in cyberspace was in accordance with the concept of 'good regulation', whereby public regulatory intervention is called for only when other, less invasive alternatives have failed[7]. However, the *Delfi* case proves that the self-regulatory approach cannot be deemed sufficient to achieve the necessary level of protection of fundamental rights if not strengthened with centrally implemented measures, as well as that Directive 2000/31/EC is clearly not enough to this end. Against this background, the *Delfi* case should encourage the debate on a new regulatory initiative on EU level that would achieve legal harmonisation in cyberspace regulation and preserve freedom of expression, thus helping the courts evade such 'slippery slopes' altogether in the future.

About the Authors

Konstantina Georgaki is an LLM candidate at the University of Cambridge, Wolfson College, and a scholar of the Onassis Foundation in Greece. She holds an LLB, an LLM in Public Law and an LLM in Private Law from the University of Athens. She has worked for an international law firm in Athens.

Emmanuel Giakoumakis is an LLM candidate at the University of Cambridge, Clare College. He holds an LLB from the University of Athens and the Diploma of International Human Rights Law of the IIDH. He interned at the Council of Europe and worked for a human rights law firm in Athens.

Alessandro Rollo is an LLM candidate at the University of Cambridge, St John's College. He holds an LLB from Roma Tre University, Rome, Italy. He interned at the US Department of Justice and the UN Office on Drugs and Crime, and worked for an international law firm.

References

[1] *Delfi AS* v *Estonia,* App no 64569/09 (ECtHR, 16 June 2015).
[2] Convention for the Protection of Human Rights and Fundamental Freedoms, art 10.
[3] 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 the Internal Market [2000] OJ L178/1, art 14-15.
[4] Case C-360/10, *SABAM v Netlog* (Judgment of the Court, Third Chamber, 16 February 2012).
[5]https://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online, 2013.
[6] *Jersild* v *Denmark,* App no 15890/89 (ECtHR, 23 September 1994), para 31.
[7] Better Regulation Task Force, Principles of Good Regulation (1998)