Intermediary Service Providers' Liability Exemptions: Where Can We Draw the Line?

Mari Männiko

Abstract The role of e-services has rapidly developed in recent years. Within these developments, the role of Internet service provider has changed from substance provider to neutral platform provider. The knowledge and control of the information available has changed from total control to no control at all. In many or we can even say in most of cases, intermediary service providers (ISPs) are not aware of information available on their service platform and therefore cannot be held responsible in the case of the breach of any rights regarding substance of information. This article analyzes the conditions on which a service provider can expect the liability exceptions to be applied. The interpretation of liability exceptions does not differ only in Member States but differ in high courts of Europe, namely in European Court of Justice (ECJ) and European Court of Human Rights (ECHR). Comparative analyses of the court reasoning show that the present legislation is too general and gives too much room for interpretation. Liability exemptions should not be applicable only on grounds of neutrality. The author believes that notice and take down principle should be implemented as a ground for exempting the liability. This article focuses on need for common approach in European level as in present situation neither ISP nor data subjects can find effective remedy to protect their interests.

1 Introduction

1.1 Scope of Analyses

This paper focuses on liability of an ISP of user-generated contents in ISP-managed platforms. The question to be answered is that to what extent is ISP responsible for data protection violations executed by uploading information concerning third parties by service users.

M. Männiko (✉)
Law Firm LEXTAL, Rävala pst 4, 10143 Tallinn, Estonia
e-mail: mari.manniko@lextal.ee

© Springer International Publishing Switzerland 2014

T. Kerikmäe (ed.), *Regulating eTechnologies in the European Union*,
DOI 10.1007/978-3-319-08117-5_7

Analyzing the court practice in Europe, the ISP liability is a question in many conflict relations (copyright and intellectual property). The applicability on liability does not depend on the right or freedom breached, and some of the judgments referred base on breach of some other right (intellectual property for instance); the main focus of this paper is on privacy violations.

Before analyzing the practice, I intend to give an overview of the legal background of the right to privacy that ISPs have to respect while providing individuals with services.

For the comparative analyses, I have chosen two European Courts, ECJ and European ECHR, whose decisions are binding for Member States.

With examples, I intend to prove that liability exceptions do not actually release ISPs from liability only due to the fact that service is listed in liability exception. The services are combined and not to be evaluated only on technical features but rather on the character of ISPs activity. Current situation does not really provide ISP with liability exceptions nor provides an individual with effective remedy in case of privacy breach.

1.2 Development Privacy-Covered Relations

Before going into details on ISP responsibility, it is important to visualize the understanding of privacy that can be violated (by ISP in this paper).

The need for common understanding of universal human rights became unavoidable after World War II. The universal right to privacy was to regulate the relationship between an individual and a state and to set minimum standards in order to prevent the abuse of power.

By the development of democracy, economical well-being and substantial raise of individualism, the privacy transformed from negative right into positive, and the right to privacy applied besides individual-state relation to individual–individual relation as well. Yet the scope was narrow. There was no Internet, and the application of the right to privacy was easy to follow.

The introduction of the Internet to the general public in early 1990s changed the world in many ways. We almost can compare the introducing of the Internet to the inventing of the printing press in terms of innovation and spreading of information.

Internet is a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a 'network of networks,' the Internet emerged in the USA in the 1970s but did not become visible to the general public until the early 1990s. By the beginning of the twenty-first century, approximately 360 million people, or roughly 6 % of the world's population, were estimated to have access to the Internet.[1]

In the context of the Internet, three situations should be distinguished that relate to personal data. The first is the publishing of elements of personal data on any Web page on the Internet. The 'Internet' comprises two main services, namely the World Wide Web and the e-mail services. While the Internet, as a network of interconnected

[1] http://www.britannica.com/EBchecked/topic/291494/Internet (last reviewed in January 31, 2014).

computers, has existed in various forms for some time, commencing with the Arpanet (United States), the freely accessible open network with www addresses and common code structure only started in the early 1990s. It seems that the historically correct term would be World Wide Web. However, given the current usage and terminological choices made in Court's case law, the word 'Internet' is primarily used to refer to the World Wide Web part of the network (the 'source Web page'). The second is the case where an Internet search engine provides search results that direct the Internet user to the source Web page. The third, more invisible operation occurs when an Internet user performs a search using an Internet search engine, and some of his personal data, such as the IP address from which the search is made, are automatically transferred to the Internet search engine service provider.[2]

Besides enormous availability of information, different ways of communication became available. New ways of information sharing and communication were introduced. Protecting privacy in the Internet became essential but not so easily achievable. Individuals were to be protected from each other but even more important from themselves. And Internet continued to develop.

While the old Web was about Web sites, clicks and 'eyeballs,' the new Web is about communities, participation and peering.[3]

To put is Simply, the old Internet (or Web) was an environment where users got together, the service provider was the owner of a server, and the control over the content provided by users was easy to handle. New Web is the environment where the contact between users is established by using service of ISP, but communication is carried out between users without ISP, sharing the content and having control over it.

The scope of privacy protected relations transformed once again, and the responsibility of platform provider, i.e., ISP, became relevant.

The dispute of liability rarely comes out when the service provided is not dubious, pure hosting, for example. The question of service provider responsibility hardly rises when one receives an insulting e-mail.

The question is more difficult to answer when the service provider provides with multi-level services, for example, a news portal provides readers with news together with the possibility to comment either anonymously or not.

1.2.1 European Convention on Human Rights Article 8: Common Grounds

The right to privacy was established and codified in European level in 1950 with ECHR of which Article 8 states that everybody has the right for respect his private and family life, his home and his correspondence.

Private life has been furnished by different aspects of privacy ever since. Starting with the question what is privacy and ending with answering where privacy can be enjoyed.

---

[2] Opinion of Attorney General Jääskinen in Case C-131/12 paragraph 3.

[3] See Tapscott and Williams (2008, p. 9).

Section 2 of the Article 8 provides with the conditions[4] under which the breach of privacy is acceptable. It is necessary to note that at the time when ECHR was adopted, the privacy protection was a state–individual relation. It was a negative right of a state not to interfere unless the precondition for interference was met. The wording of Article 8 has remained the same, but the substance has transformed by the court practice besides the individual–state relation to the individual–individual relation, and the contracting state has to provide an individual with an effective remedy for privacy protection.

1.2.2 Charter on Fundamental Rights of European Union

It was a remarkable development regarding the uniform implementation of fundamental rights within European Union. Most importantly, the right to data protection was separated from general protection of privacy. The right to data protection was no longer a part of the right to privacy, but it became an individually protected value. In substance, nothing really changed.

According to Advocate General Jääskinen[5] *this fundamental right, being a restatement of the European Union and Council of Europe acquis in this field, emphasises the importance of protection of personal data, but it does not as such add any significant new elements to the interpretation of the Directive.*[6]

1.2.3 Data Protection Directive 95/46/EC

As mentioned before, Internet became commonly available in early 1990s, and by 1995, European Union introduced the first[7] framework act to unify data protection laws in EU.

Data Protection Directive[8] established several new principles and instruments, but in the present paper, I would like to point out the individuals' right to have

[4] There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[5] In his opinion the the case of European Court of Justice no C-131/12 paragraph 113.

[6] Data Protection Directive 95/46/EC.

[7] The Directive can be called first in European Union but it is surely not the first act that separated data protection from the rest of privacy protection. Outstanding codification has be en done before. In September 23, 1980 OECD adopted Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In 1981 European Council adopted Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. According to this Convention tozens of recommendations have been adopted.

[8] Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred as to Data Protection Directive).

control over his/her personal data to be processed by third persons, and the institute of consent for data processing.

In relations with ISP, it is also important to know how and if the consent for data processing is achieved and if the data subject is informed about the possibility not to give consent knowingly.

ISP services and relations with the users of services are very different. From the perspective of Data Protection Directive, it is important to define if the ISP is a data controller and if activities of an ISP can be defined as data processing. The answer to those questions is the fact if an ISP can influence the data flow and the substance of the data.

1.2.4 E-Commerce Directive 2000/31/EC

E-Commerce Directive[9] gave a definition of ISP as well as limited service providing from other possible activities done in Internet.

Information Society Services (hereinafter ISS) is a service that must meet the following conditions according to E-Commerce Directive Article 2(a).

Article 2 of the E-Commerce Directive uses the definition contained in Article 1(2) of Directive 98/34/EC[10] as amended by Directive 98/48/EC[11]; ISS is a service normally provided for remuneration, at a distance, by electronic means and at the individual request.

Privacy can be affected when an individual uses an information society service, in particular for the purposes of seeking information or making it accessible.

Distinction of the Activities Listed in Liability Exceptions of the E-Commerce Directive

The liability exceptions derive from Section 4 (Articles 12–15) of the E-Commerce Directive.

ISP who provide with intermediary services liability is limited. The keywords for liability limitations are 'mere conduit,' 'caching' and 'hosting.'

Mere conduit means that ISP does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission.

---

[9] E-Commerce 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 ('Directive on electronic commerce') (hereinafter E-Commerce Directive).

[10] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations.

[11] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. Last reviewed at January 29, 2014.

Caching means that ISP activities are performed exclusively for more efficient onward transmission of the information to other recipients of the service upon such recipients' requests.

Hosting means that ISP is storing information without monitoring the substance of it.

According to the functional character of information society services, they can be distinguished as follows:

- Hosting service provider provides users with the possibility to make the content available using service providers server(s). The server can be used by content providers and third persons. A distinction may be established between caching, where the purpose of hosting is to facilitate the functioning of the network through automatic, intermediate and transient storage of information, and hosting, that is, commercial or other storage that is permanent or more than merely provisional.[12]
- Access service provider connects service users computer to Internet.
- A transit service provider provides service users with possibility to transfer data (*mere conduit*)

The E-Commerce Directive (Article 15) sets general rule that ISP who provides its users with the platform does not have the general obligation to monitor the data shared by service users. The analyses of the case law show that there are certain limitations to that rule.

2 ISP Liability Exceptions According to Law and Practice of ECJ and ECHR

According to several judgments of ECJ in order to benefit from liability exemptions, ISP has to prove the lack of control and knowledge over the information processed on its platform. At the same time, ECJ gives controversial meaning to neutrality and seems that within the court there is no consensus about the substance and applicability of being neutral.

2.1 Google Case

The dispute in Google versus Louis Vuitton and the others[13] concerned the display on the Internet of advertising links on the basis of keywords corresponding to

[12] Gallardo Claudio Ruiz and Gálvez J. Carlos Lara Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America available at http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf. Last reviewed at January 30, 2014.

[13] Joined Cases C-236/08 to C-238/08.

trademarks and the question taken to the ECJ was if the liability exemptions from E-Commerce Directive Articles 12–14 apply to Google.

Google operates an Internet search engine. When an Internet user performs a search on the basis of one or more words, the search engine will display the sites, which appear best to correspond to those words, in decreasing order of relevance. These are referred to as the 'natural' results of the search.

Besides natural results which Google provides with advertising link that provides the user with commercial announcements. Natural and commercial results are easily distinguished.

The question taken to the ECJ was whether Google is responsible for intellectual property infringements or will liability exceptions applying due to the character of services provided by Google. From perspective of this paper, only the latter is important.

The ECJ had the occasion to give its interpretation in the case; the ECJ interpreted the role of the host service according to recital 42 of the preamble of the E-Commerce Directive. The exemptions from liability established in that directive cover only cases in which the activity of the information society service provider is 'of a mere technical, automatic and passive nature,' which implies that that service provider 'has neither knowledge of nor control over the information which is transmitted or stored.'[14]

Article 14 of the Directive 2000/31 must be interpreted as meaning that the rule laid down therein applies to an Internet-referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned.[15]

In his opinion, the Advocate General Poiares Maduro pointed out a need for common notice and take down principle adaption for attribution of liability following the taking down of content.

The ECJ found that the services of Google can be interpreted according to the exceptions provided by the E-Commerce Directive and Google cannot be held liable.

2.2 L'Oreal Versus eBay

The dispute in L'Oreal versus eBay[16] the main proceedings was between L'Oréal SA and its subsidiaries ('L'Oréal'), on the one hand, and three subsidiaries of

[14] Viola de Azevedo Cunha, Mario, Martin, Luisa, Sarator, Giovanni EUI Working Paper Law 2011/011. Department of Law, Peer-to-peer privacy violations and ISP Liability: Data protection in the User/Generated WEB p. 6.

[15] Judgement in Joined Cases C-236/08 to C-238/08.

[16] European Court of Justice, Case C-324/09.

eBay Inc. ('eBay'), together with certain natural persons, on the other. It related to offers for sale of goods by these persons on eBay's electronic marketplace. The offers for sale allegedly infringed L'Oréal's intellectual property rights.

eBay, the defendant in the national proceedings, operates a popular and sophisticated electronic marketplace in the Internet. It has built-up a system, which greatly facilitates the selling and buying over the Internet by individuals, with a powerful search engine, a secure payment system and extensive geographical coverage. It has also designed compliance mechanisms to fight sales of counterfeit goods. In order to attract new customers to its Web site, eBay has also bought keywords, such as well-known trademarks, from paid Internet-referencing services (such as Google's AdWords). The use of a selected keyword in the search engine triggers the display of an advertisement and a sponsored link, which leads directly to eBay's electronic marketplace.[17]

eBay has installed a notice and take down system that is intended to assist intellectual property owners in the removing of the infringing listings from the marketplace.

The question to be answered is whether eBay can be held liable for the infringements.

ECJ had to define the scope of the exemption of the information service providers' liability as contained in Article 14 of the Directive 2000/31 ('E-Commerce Directive').

ISP's role in the data processing is the determining factor. Does ISP have knowledge of, or control over, the data stored. If the role can be defined as passive, i.e., no knowledge nor control, the service provider cannot be held liable for the data which it has stored.

In the case of *L'Oreal versus eBay*, the meaning of 'neutrality' was analyzed by Advocate General Jääskinen in his opinion.

Advocate General contended that the liability exceptions should apply, but he had doubts whether neutrality should be the right test under the E-Commerce Directive for applying the exemptions.

When anchoring the limitation of liability criteria of the hosting provider to 'neutrality,' the Court has referred to recital 42 of the Directive 2000/31. I share the doubts expressed by eBay as to whether this recital 42 at all concerns hosting referred to in Article 14.

Even if recital 42 of the directive speaks of 'exemptions' in plural, it would seem to refer to the exemptions discussed in the following recital 43. The exemptions mentioned there concern—expressly—'mere conduit' and 'caching.' When read this way, recital 42 becomes clearer: it speaks of 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.' In my view, this refers precisely to 'mere conduit' and 'caching,' mentioned in Articles 12 and 13 of the Directive 2000/31.

[17] Ibid, paragraph 2.

Rather, it is recital 46 which concerns hosting providers mentioned in Article 14 of the Directive 2000/31, as that recital refers expressly to the storage of information. Hence, the limitation of liability of a hosting provider should not be conditioned and limited by attaching it to recital 42. It seems that if the conditions set out in Google France and Google for a hosting provider's liability are confirmed in this case to apply also to electronic marketplaces, an essential element in the development of electronic commerce services of the information society, the objectives of the Directive 2000/31 would be seriously endangered and called into question.[18]

Moreover, Jääskinen highlights that he *would find it surreal that if eBay intervenes and guides the contents of listings in its system with various technical means, it would by that fact be deprived of the protection of Article 14 regarding storage of information uploaded by the users.*[19] *The Advocate General suggests that it is possible to sketch out parameters of a business model that would fit perfectly to the hosting exemption. And even if it were, a definition made today would probably not last for long. Instead, we should focus on a type of activity and clearly state that while certain activities by a service provider are exempt from liability, as deemed necessary to attain the objectives of the directive, all others are not and remain in the 'normal' liability regimes of the Member States, such as damages liability and criminal law liability.*[20]

Therefore, when it is accepted that certain activities by a service provider are exempted that means conversely that activities not covered by an exemption may lead to liability under national law.

Thus, for eBay, the hosting of the information provided by a client may well benefit from an exemption if the conditions of Article 14 of Directive 2000/31 are satisfied. Yet the hosting exception does not exempt eBay from any potential liability, it may incur in the context of its use of a paid Internet-referencing service.[21]

Mario Viola De Azevedo Cunha and other authors believe that the interpretation of the provider's exemption given by Advocate General Jääskinen could fall under neutrality broadly understood, which applies to an activity which is meant to enable or facilitate the activities in which the user autonomously engages in his or her own behalf. The Advocate General urges us to rethink the foundations of the liability exemption. We should consider the specific activity performed by an ISP and understand neutrality as appropriateness with regard to the purpose of that activity.[22]

According to Mario Viola de Azevedo Cunha, the neutral activity of the providers should be exempted from the liability also with regard to national data protection rules.

---

[18] Paragraphs 130–165.

[19] Paragraph 146.

[20] Paragraph 149.

[21] Paragraphs 150–151.

[22] Viola de Azevedo Cunha, Mario, Martin, Luisa, Sarator, Giovanni, EUI Working Paper Law 2011/011. Department of Law, Peer-to-peer privacy violations and ISP Liability: Data protection in the User/Generated WEB p. 7–8.

Attorney General Jääskinen gave his view on the notion of notice and take down as following.

It should be recalled that Article 14(1)(b) of the Directive 2000/31[23] reflects the principle of *notice and take down*. Accordingly, the hosting provider has to act expeditiously to remove or to disable access to the illegal information upon obtaining actual knowledge of the illegal activity or illegal information or awareness of facts or circumstances from which the illegal activity or information is apparent.

In the application of the principle of *notice and take down*', recital 46 of the Directive 2000/31 must be taken into account. According to it, 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. Moreover, the directive does not affect Member States' possibility of establishing specific requirements, which must be fulfilled expeditiously prior to the removal or disabling of information.[24]

The Court took a different approach on neutrality in case of eBay and found that Article 14(1) of the E-Commerce Directive is to be interpreted as applying to the operator of an online marketplace where that operator has not played an active role allowing it to have knowledge or control of the data stored. The operator plays such a role when it provides assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting them.[25]

ECJ found that the operator has provided assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer–seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of the Directive 2000/31.[26]

2.3 Scarlet Extended SA

Scarlet Extended SA[27] is an Internet service provider, which provides its customers with access to the Internet without offering other services such as downloading or file sharing.

SABAM is a management company that represents authors. SABAM concluded that Internet users using Scarlet's services were downloading works in SABAM's catalogue from the Internet, without authorization and without paying

[23] E-Commerce Directive.

[24] Opinion of Attorney General Jääskinen in Case C-324/09.

[25] European Court of Justice, Case C-324/09: paragraph 123 of the judgment.

[26] Ibid, paragraph 116.

[27] Judgement of the Court, In Case C-70/10.

royalties, by means of peer-to-peer networks, which constitute a transparent method of file sharing which is independent, decentralized and features advanced search and download functions.

SABAM claimed that Scarlet had infringed copyrights and sought an order requiring Scarlet to bring such infringements to an end by blocking, or making it impossible for its customers to send or receive in any way, files containing a musical work using peer-to-peer software.

At the same time, the filtering and blocking system required by SABAM for the protection of intellectual property rights would be in conflict with E-Commerce Directive principle that the service provider cannot be obliged to monitor the substance of data.

Scarlet claimed that such an injunction was contrary to Article 21 of the Law of 11 March 2003 on certain legal aspects of information society services, which transposes Article 15 of Directive 2000/31 into national law, because it would impose on Scarlet, de facto, a general obligation to monitor communications on its network, inasmuch as any system for blocking or filtering peer-to-peer traffic would necessarily require general surveillance of all the communications passing through its network. Scarlet considered that the installation of a filtering system would be in breach of the provisions of European Union law on the protection of personal data and the secrecy of communications, since such filtering involves the processing of IP addresses, which are personal data.

The question put to the court were, whether the E-Commerce Directive and the Data Protection Directive among other directives (2001/29, 2004/48 and 2002/58), read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction imposed on an Internet service provider to introduce a system for filtering all electronic communications passing via its services, in particular those involving the use of peer-to-peer software, which applies indiscriminately to all its customers, as a preventive measure, exclusively at its expense and for an unlimited period which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audiovisual work in respect of which the applicant claims to hold intellectual property rights, with a view to blocking the transfer of files the sharing of which infringes copyright ('the contested filtering system').[28]

The ECJ found that all rules must respect Article 15(1) of the E-Commerce Directive, which prohibits national authorities from adopting measures, which would require an Internet service provider to carry out general monitoring of the information that it transmits on its network.

The Court has already ruled that that prohibition applies in particular to national measures which would require an intermediary provider, such as an ISP, to actively monitor all the data of each of its customers in order to prevent any future infringement of intellectual property rights. Furthermore, such a general

[28] Ibid, paragraph 29.

monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly.

Firstly, the filtering system would require the ISP to identify, within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic, secondly, to identify, within that traffic, the files containing works in respect of which holders of intellectual property rights claim to hold rights, thirdly, to determine which of those files are being shared unlawfully, and fourthly, to block file sharing that it considers to be unlawful.

ECJ found that the abovementioned must be interpreted as an obligation to monitor such activities according to the Article 15 of the E-Commerce Directive.

As for the data protection rights, ECJ found that it is the common ground that the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content, and the collection and identification of users' IP addresses from which unlawful content on the network are sent. Addresses are personal data because they allow those users to be identified.

The answer to the questions submitted is that the E-Commerce Directive, the Data Protection Directive and Directives 2001/29, 2004/48 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against an ISP, which requires it to install the contested filtering system.

The ECJ found that ISP must not be held liable for the infringement of rights on its platform.[29]

2.4 Google Spain SL, Google Inc. Versus Agencia Española de Protección de Datos and Mario Costeja Gonzáles

The proceedings concerned the application of the Data Protection Directive to an Internet search engine that Google operates as service provider. In the national proceedings, it is undisputed that some personal data regarding the data subject have been published by a Spanish newspaper, in two of its printed issues in 1998, both of which were republished at a later date in its electronic version made available on the Internet. The data subject thought that this information should no longer be displayed in the search results presented by the Internet search engine operated by Google, when a search is made of his name and surnames.[30]

The questions referred to the Court fell into three categories. The first group of questions related to the territorial scope of the application of EU data protection rules. The second group addressed the issues relating to the legal position of an Internet search engine service provider. Finally, the third question concerned the

[29] The ECJ came to the same conclusion as in the case C-360/10.

[30] Opinion of Advocate General Jääskinen delivered on 25 June 2013 (1) Case C-131/12.

so-called right to be forgotten, and the issue of whether data subjects can request that some or all search results concerning them are no longer accessible. All of these questions were new to the Court.

It is useful to review the opinion of ECJ about the liability of ISP for not providing data subject with the right to be forgotten.

It is necessary to analyze their position vis-à-vis the legal principles underpinning the limitations on the liability of Internet service providers. In other words, to what extent are activities performed by an Internet search engine service provider, from the point of view of liability principles, analogous to the services enumerated in the E-Commerce Directive 2000/31 (transfer, mere caching, hosting) or transmission service mentioned in recital 47 in the preamble to the Directive, and to what extent does the Internet search engine service provider act as content provider in its own right.[31]

Here is no doubt that the newspaper who is keeping the old articles about data subject available is a data processor in the meaning of Data Protection Directive. The question to be answered is whether and to what extent Google is liable or is the liability to be excluded by exceptions.

It is important to examine the liability of Internet search engine service providers in respect of personal data published on third-party source Web pages, which are accessible through their search engines. In other words, the Court is here faced with the issue of 'secondary liability' of this category of information society service providers analogous to that it has dealt with in its case law on trademarks and electronic marketplaces.[32]

The Internet search engine service provider merely supplying an information location tool does not exercise control over personal data included on third-party Web pages. The service provider is not 'aware' of the existence of personal data in any other sense than as a statistical fact Web pages are likely to include personal data. In the course of processing of the source Web pages for the purposes of crawling, analyzing and indexing, personal data do not manifest itself as such in any particular way.[33]

Attorney General Jääskinen is of the opinion that ISP cannot be held a data controller due to the technical character of its services, and it meets all the essential requirements of the liability exemption. Besides the E-Commerce Directive, the liability for personal data processing is excluded by the recital 47 in the preamble of the Data Protection Directive.[34]

---

[31] Ibid, paragraph 38.

[32] Ibid, paragraph 46.

[33] Ibid, paragraph 84.

[34] Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services.

If a data subject finds that his rights are breached by continuous availability of his personal data, he must find a legal ground for stopping the processing at the original data processor (newspaper in this case); as ISP is not responsible neither for the fact that data has been processed nor for the substance of the data.

In this case, ECJ gave opinion on notice and take down concept and found that a national data protection authority cannot require an Internet search engine service provider to withdraw information from its index except for the cases where this service provider has not complied with the exclusion codes or where a request emanating from the Web site regarding update of cache memory has not been complied with. A possible *notice and take down* procedure concerning links to source Web pages with illegal or inappropriate contents is a matter of national law civil liability based on grounds other than the protection of personal data.

ECJ refers to Article 29 Data Protection Working party Opinion 1/2008 on data protection issues related to search engines according to which the formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers. With regard to the removal of personal data from their index and search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases, but the extent to which an obligation to remove or block personal data exists may depend on the general tort law and liability regulations of the particular Member State. In some EU Member States, data protection authorities have specifically regulated the responsibility of search engine providers to remove content data from the search index, based on the right of objection enshrined in Article 14 of the Data Protection Directive and on the E-Commerce Directive. According to such national legislation, search engines are obliged to follow a notice and take down policy similar to hosting providers in order to prevent liability.

2.5 Conclusion on ECJ Judgments

According to the rule that is generally adopted by ECJ, an ISP is not liable if it has neutral and technical role. Neutral means not having influence on data or on conditions on which data are available at ISP's platform. ISP is not liable in case it is not a data controller.

The substance of neutrality is subjective, and ECJ has not reached the consensus on the question if neutrality should be unconditional.

Either in judgments or opinions of attorney General the ECJ has pointed out the need for common approach for adapting notice and take down principle and its effect to liability.

As the First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal

Market (Directive on electronic commerce)[35] noted the notice and take down principle was to be adopted on self-regulatory principles on the discretion of Member States.

The time has shown that self-regulation is not sufficient and the principle should be adopted in Member States' national legislation in order for it to become an effective remedy in case of violations and for balancing the liability.

2.6 Delfi Versus Estonia

The applicant company owned one of the largest Internet news portals in Estonia. On its Web site, readers could anonymously and without prior registration post comments below the published articles. Although the applicant company could not edit or moderate such comments, it could remove them using a prior automatic word filtering system or on being alerted by readers.

There was a system of notify-and-take-down in place: Any reader could mark a comment as appropriate and the comment was removed expeditiously. Furthermore, there was a system of automatic deletion of comments that included obscene words. In addition, a victim of a defamatory comment could directly notify the applicant company, in which case the comment was removed immediately.

In 2006, the applicant published an article stating that a ferry company had changed its routes thereby causing the breakup of ice at potential locations of ice roads. As a result, the opening of the roads—which were a cheaper and faster connection to the Estonian islands compared to the company's ferry services—had to be postponed for several weeks. A number of comments containing personal threats and offensive language directed against the ferry company owner were posted below the article. The applicant company removed them some 6 weeks later at the insistence of the ferry company. The owner of the ferry company instituted defamation proceedings against the applicant company, which was ultimately ordered to pay EUR 320 in damages.

The Information Services Act[36] (adopted under E-Commerce Directive) limits ISP responsibility on the same grounds as E-Commerce Directive, i.e., ISP will not be held responsible for the content in case the service consists of mere conduit, caching or hosting. The same as in E-Directive there is no obligation to monitor.

The Supreme Court approved the lower courts' interpretation of the Information Society Services Act and reiterated that an ISP, falling under that Act and the Directive on Electronic Commerce, had neither knowledge of nor control

[35] First Report on the application of 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 (Directive on electronic commerce).

[36] https://www.riigiteataja.ee/akt/106012011012.

over information, which was transmitted or stored. By contrast, a provider of content services governed the content of information that was being stored. In the present case, the Delfi had integrated the comment environment into its news portal and invited users to post comments. The number of comments had an effect on the number of visits to the portal and on the applicant company's revenue from advertisements published on the portal. Thus, the applicant company had an economic interest in the comments. The fact that the applicant company did not write the comments itself did not imply that it had no control over the environment. It enacted the rules of commenting and removed comments if the rules were breached. The users, on the contrary, could not change or delete the comments they had posted; they could merely report obscene comments. Thus, the applicant company could determine which comments were published and which not. The fact that it made no use of this possibility did not mean that it had no control over the publishing of the comments.

The Court found that the services of Delfi do not fall under scope of exemptions of E-Commerce Directive and relevant local act and Delfi was held responsible on general principles of tort law.

ECHR noted that the interpretation of local law is the task of local courts and as Estonian Courts ruled that Delfi's activities do not fall under exceptions provided by E-Commerce Directive and relevant local law the ECHR will not take the task of local courts and will not start re-interpretation.

The ECHR reviewed the case law (analyzed above) and found that the neutrality principle that was essential in findings of ECJ was of no relevance in this case as ECHR relied on interpretation of Estonian courts regarding applicability of neutrality.

ECHR found that there was infringement with Article 10[37] of European Convention on Human Rights (hereinafter the Convention), but the exercise of this freedom was restricted by the law with sufficient amount of foreseeability.

The parties' views differed as to whether the applicant company's civil liability for the defamatory comments amounted to a disproportionate interference with its freedom of expression. In other words, the question is whether the applicant company's obligation, as established by the domestic judicial authorities, to ensure that comments posted on its Internet portal did not infringe the personality rights of third persons was in accordance with the guarantees set out in Article 10 of the Convention.[38]

[37] Article 10. Freedom of expression. 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[38] Paragraph 84.

As regards the measures applied by the applicant company, the Court notes that, in addition to the disclaimer stating that the writers of the comments—and not the applicant company—were accountable for them and that it was prohibited to post comments that were contrary to good practice or contained threats, insults, obscene expressions or vulgarities, the applicant company had two general mechanisms in operation. Firstly, it had an automatic system of deletion of comments based on stems of certain vulgar words. Secondly, it had a notice and take down system in place according to which anyone could notify it of an inappropriate comment by simply clicking on a button designated for that purpose, to bring it to the attention of the portal administrators. In addition, on some occasions, the administrators of the portal removed inappropriate comments on their own initiative. Thus, the Court considered that the applicant company could not be said to have wholly neglected its duty to avoid causing harm to third parties' reputations. Nevertheless, it was discovered that the automatic word-based filter used by the applicant company was relatively easy to circumvent. Although it may have prevented some of the insults or threats, it failed to do so in respect of a number of others. Thus, while there is no reason to doubt its usefulness, the Court considers that the word-based filter as such was insufficient for preventing harm being caused to third persons.[39]

The ECHR considered that the applicant company exercised a substantial degree of control over the comments published on its portal even if it did not make as much use as it could have done of the full extent of the control at its disposal.

The author believes that as the ECHR found that Delfi had a control over the comments and monitored the comments to some extent, it could not be held neutral and the liability exemptions from the E-Commerce Directive could not apply.

The ECHR found that Article 10 of the Convention was not violated.

2.7 Case of Yildirim Versus Turkey

The applicant owns and runs a Web site on which he publishes material including his academic work. It was set up using the Google Sites Web site creation and hosting service. On June 23, 2009, the Criminal Court of First Instance ordered the blocking of another Internet site under the Law on regulating publications on the Internet and combating Internet offences. The order was issued as a preventive measure in the context of criminal proceedings. Later that day, under the same Law, a copy of the blocking order was sent to the Telecommunications Directorate for execution. On June 24, 2009, further to a request by the Telecommunications Directorate, the Criminal Court of First Instance varied its decision and ordered the blocking of all access to Google Sites. As a result, the applicant was unable to access his own site. On July 1, 2009, he applied to have the blocking order set

[39] Ibid, paragraph 87.

aside in respect of his own site, which had no connection with the site that had been blocked because of its illegal content. On July 13, 2009, the Criminal Court dismissed the applicant's application. In April 2012, he was still unable to access his own Web site even though, as far as he understood, the criminal proceedings against the owner of the offending site had been discontinued in March 2011.[40]

Following the blocking of another Web site as a preventive measure, the court had subsequently, further to a request by the Telecommunications Directorate, ordered the blocking of all access to Google Sites, which also hosted the applicant's site. This had entailed a restriction amounting to interference with the applicant's right to freedom of expression.

The blocking of the offending site had a basis in law, but it was clear that neither the applicant's site nor Google Sites fell within the scope of the relevant law since there was insufficient reason to suspect that their content might be illegal. No judicial proceedings had been brought against either of them. Furthermore, although Google Sites were held responsible for the content of a site it hosted, the law made no provision for the wholesale blocking of access to the service. Nor was there any indication that Google Sites had been informed that it was hosting illegal content or that it had refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings. Furthermore, the law had conferred extensive powers on an administrative body, the Telecommunications Directorate, in implementing a blocking order since it had been able to request an extension of the scope of the order even though no proceedings had been brought in respect of the site or domain concerned and no real need for wholesale blocking had been established.[41]

ECHR referred to a decision of ECJ (see Section 2.1.4 of the article) which found that imposing ISP with an obligation to filter the content provided on its platform is to be interpreted as an obligation to monitor that is in contrary with E-Commerce Directive and breaches fair balance between the rights.

Besides that ECHR analyzed practices in Council of Europe Member States and finalized that freedom of expression protected by Article 10 of the Convention implied freedom of access to Internet.

Although Google was not a part of the proceeding and it was not a subject matter if ISPs rights have been violated by Turkish Court order, the ECHR took approach on ISP liability as well. The ECHR noted that neither Google Sites nor the applicant's Web site was the subject of judicial proceedings for the purposes of relevant national laws. It appears from national court decision that Google Sites were held to be liable for the content of a Web site which it hosted. However, the national law, which deals with the liability of content providers, hosting service providers and access providers make no provision for a wholesale blocking of access such as that ordered in the present case.

[40] Information Note on the Court's case-law No. 158.

[41] Ibid.

Nor has it been maintained that the law authorized the blocking of an entire Internet domain-like Google Sites, which allows the exchange of ideas and information. Moreover, there is nothing in the case file to indicate that Google Sites were notified under that it was hosting illegal content, or that it refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings.

ECHR found that there has been a breach of Article 10 of the Convention.

3 Conclusion

Neutrality in the meaning of the E-commerce Directive liability exemptions means passive role and not knowing or adapting conditions to the data processed at the platform.

Liability exemptions should not be applicable only on grounds of neutrality. Implementing sole neutrality clause may bring along unwillingness of ISP to interfere, and it affects the protection of personal rights on the ISPs platform.

Liability exceptions should be applied in case an ISP acts promptly after being informed about a breach of law (notice and take down principle).

The conditions under which a hosting provider is exempted from liability, as set out at Article 14(1)(b) constitute the basis for the development of notice and take down procedures for illegal and harmful information by stakeholders. Article 14 applies horizontally to all types of information.

In the year 2000, when the Directive was adopted, it was believed that notice and take down procedures do not have to be regulated in the E-Commerce Directive as it was hoped that the self-regulation is sufficient as Article 16 and Recital 40 of the E-Commerce Directive expressly encourage it.

This approach was followed by the Member States in their national laws. Out of those Member States which have transposed the Directive, only Finland has included a legal provision setting out a notice and take down procedure concerning copyright infringements only. All the other Member States have left this issue to self-regulation.[42]

Cases analyzed above prove that self-regulation has failed in the case of protection of privacy[43] in ISP platforms. The E-Commerce Directive should implement regulation for notice and take down procedure in order to have an effective remedy for the protection of rights on ISP platforms.

---

[42] First Report on the application of 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 (Directive on electronic commerce). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF. Last reviewed at January 29, 2014.

[43] The same as protecting copyright, intellectual property etc.

References

Book, Multiple Authors/Editors

Tapscott, D., & Williams, A. D. (2008) *Wikinomics: How mass collaboration changes everything* (p. 19). New York: Portfolio.

Journal Articles

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations.

Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

E-Commerce 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 ('Directive on electronic commerce').

Gallardo Claudio Ruiz, & Gálvez J. Carlos Lara, Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America available at http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/02-Liability_Internet_Service_Providers_exercise_freedom_expression_Latin_America_Ruiz_Gallardo_Lara_Galvez.pdf.

Viola de Azevedo Cunha, Mario, Martin, Luisa, Sarator, Giovanni, EUI Working Paper Law 2011/011. Department of Law, Peer-to-peer privacy violations and ISP Liability: Data protection in the User.

Online Documents

Article 10: Right to freedom of expression.

Information Note on the Court's case-law No. 158.

Internet—http://www.britannica.com/EBchecked/topic/291494/Internet.

First Report on the application of 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 (Directive on electronic commerce). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF.

https://www.riigiteataja.ee/akt/106012011012.

Court Decisions

European Court of Justice no. C-131/12 paragraph 113.

European Court of Justice, Case C-324/09.

European Court of Justice, Case C-324/09: paragraph 123 of the judgment.
Judgement in Joined Cases C-236/08 to C-238/08.
Judgement of the Court In Case C-70/10.
Opinion of Attorney General Jääskinen in Case C-131/12 paragraph 3.
Opinion of Attorney General Jääskinen in Case C-324/09.