**TALLINN UNIVERSITY OF TECHNOLOGY**

Faculty of Social Sciences

Tallinn Law School

Kadi Avingo

# Intermediary Liability for User-Generated Content in Europe

Master thesis

Supervisor: Lecturer Addi Rull, LL.M.

Tallinn 2016

## Table of Abbreviations

AG – Advocate General

Art 29 WP – Article 29 Working Party (the group of EU data protection authorities)

CDA – Communications Decency Act (United States)

CJEU – Court of Justice of the European Union

CoE – Council of Europe

DMCA – Digital Millennium Copyright Act (United States)

DPA – Data Protection Authority

DPD – Data Protection Directive

ECD – e-Commerce Directive

ECHR – Convention for the Protection of Human Rights and Fundamental Freedoms

ECtHR – European Court of Human Rights

EUCFR – Charter of Fundamental Rights of the European Union

GDPR – General Data Protection Regulation

ICCPR – International Covenant on Civil and Political Rights

ISSA – Information Society Services Act (Estonia)

LCEN – the French e-Commerce Act

NTD – notice and take-down

IP – internet protocol

IPR – intellectual property rights

ISP – internet service provider

OECD – Organisation for Economic Co-operation and Development

RTBF – the right to be forgotten

UDHR – Universal Declaration of Human Rights

UGC – user-generated content

## Table of Contents

## Introduction

In the era of Web 2.0, most of the content available online is user-generated. „We're all participating in the rise of a global, ubiquitous platform for computation and collaboration that is reshaping nearly every aspect of human affairs. While the old Web was about Web sites, clicks, and 'eyeballs', the new Web is about the communities, participation and peering. As users and computing power multiply, and easy-to-use tools proliferate, the Internet is evolving into a global, living, networked computer that anyone can program."[1] Thus, internet has become a forum where everyone can exercise their civil, economic and political rights, and where one can develop one's social personality and engage in social relationships. The role of the internet as a fundamental enabler of individual and social development is not, however, always socially beneficial as evidenced by defamation, violation of intellectual property rights, hate speech, child pornography, support of criminal activity and terrorism, etc. Most user-generated content (UGC), whether beneficial or not, is supported by the activities of profit-seeking private companies, who provide the infrastructure necessary for the exercise of their users' rights.[2] These are internet intermediaries, who form the main subject matter of the present thesis.

The nature and functions of intermediaries sometimes vary significantly, ranging from providing basic telecommunications services to storing and making available all types of information emanating from their users. Examples include internet access providers, operators of video services, online marketplaces and auctions, video and photo sharing websites, operators of blogs and microblogs, as well as discussion forums, collaborative websites, such as Wikipedia, software distribution websites, news aggregation services, and so on. Their one common feature is that they act as gatekeepers between the participants on the internet, and do not themselves create the content they transmit or store. Through this gatekeeper role, intermediaries fulfil an essential function in the online dissemination of information.[3]

Due to this role, and despite the warnings of John Perry Barlow in his 1996 Declaration of the Independence of Cyberspace telling governments, "the weary giants of flesh and steel", to leave

[1] Tapscott, D. & Williams, A.D. Wikinomics: How Mass Collaboration Changes Everything. New York: Penguin New York 2008, p. 19
[2] Azevedo Cunha, M. V., Marin, L. & Sartor, G. Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web (2012) International Data Privacy Law, Vol. 2, No. 2, at 51
[3] Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' *Common Market Law Review* 48: 1455-1502, 2011, at 1455

the internet alone and free of the tyrannies of laws and regulations, they have not listened.[4] Governments around the world are increasingly pressuring intermediaries to block their users' unlawful, or merely undesired content in order to suppress dissent, hate speech, privacy violations, etc. One way of doing so is holding the intermediaries legally responsible for the actions of their users.[5] The current thesis provides an overview of the legal framework governing the liability of internet intermediaries in the EU. Currently, in Europe, there seem to be three separate regimes that govern the liability of internet intermediaries for content created by their users. These are the e-Commerce Directive, the Data Protection Directive and the freedom of expression. Although each regime seemingly has their own specific field of application, they also tend to overlap, which has resulted in legal uncertainty, inequality and confusion since each system creates specific obligations for internet intermediaries.

The research has been conducted using the qualitative research method, with a focus on analysing the European legal order, stemming from the European Union and the Council of Europe. Thus, discussion and analysis primarily rest on EU and Council of Europe legislation and the corresponding national instruments, as well as case law, mainly from the Court of Justice of the European Union and the European Court of Human Rights, although some decisions of national courts of the EU Member States are also included.

The hypothesis of the thesis is that the current state of intermediary liability for user-generated content in the European legal order is extremely unclear since there are three separate and conflicting regimes that simultaneously govern the issue. The primary aim to be achieved with the research is to examine and determine how current European legislation and case law responds to the issue of intermediary liability, especially in cases involving user-generated content, and to draw comparisons between the different regimes and to analyse their effects.

The research questions of the thesis are:

1. Does the case law of the European courts indicate that there are three different and incompatible regimes applicable to intermediary liability in Europe or can they in fact be reconciled with each other?

[4] Barlow, J.P. A Declaration of the Independence of Cyberspace (Davos, February 8, 1996) https://www.eff.org/cyberspace-independence (12.12.2015)
[5] Keller, D. Intermediary Liability. http://cyberlaw.stanford.edu/focus-areas/intermediary-liability (11.11.2015)

2. Under what conditions should an internet intermediary be held liable for user-generated content and what kind of precautionary measures would it be reasonable to require intermediaries to take in order to avoid such liability?
3. What are the potential effects of holding intermediaries liable for user-generated content on freedom of expression, anonymity, and freedom to conduct a business?

The present thesis proceeds in five main chapters. The first deals with the past, by defining the concept and roles of online intermediaries and giving an historical overview of the legislative and regulatory frameworks concerning the liability of internet intermediaries. The following three chapters deal with the present, by providing an examination of the current state of the law (*lex lata*) in the European legal order. Accordingly, the second chapter covers the liability of internet intermediaries under the regime of the e-Commerce Directive, the third chapter assesses their position under the Data Protection Directive, and the fourth chapter analyses the application of the fundamental right to freedom of expression to intermediary liability. The fifth chapter examines the circumstances in which the three aforementioned regimes overlap and attempts to shine a light on the future developments and direction of intermediary liability (*lex ferenda*).

# 1. Intermediary Liability

The internet is often described as a giant network of networks created to carry, host and index information, content and services. This information is distributed, hosted and transmitted by internet intermediaries, whose role in the whole enterprise of the information society is therefore essential.[6] Although at first glance the meaning of the term intermediary may seem rather straightforward, in practice, numerous internet actors with sometimes significantly contrasting roles and activities have been grouped under this heading. Furthermore, several other terms have emerged instead of intermediary, therefore making it necessary to clarify the exact subject matter of the present thesis.

## 1.1. Definition of an Internet Intermediary

The Organisation for Economic Co-operation and Development (OECD) defines internet intermediaries based on their functions, namely connecting or facilitating transactions between third parties on the internet since they provide access to, host, transmit and index content and services coming from third parties on the internet or provide internet-based services to third parties. The word intermediary signifies the position between or among two or more parties, and although intermediaries aid the transmission process, they do not, at least in most cases, initiate or make decisions to disseminate the content or services that travel across their networks or servers.[7]

The prevailing types of intermediaries are internet service providers (ISPs), web hosting providers, social media platforms and search engines. ISPs, also referred to as access providers, control the physical infrastructure required to access the internet and make this service available to customers for a fee. Hosting providers originally only included companies that rent web server space to allow their customers to set up their own websites, but nowadays the term covers any actor that controls a website which allows third parties to upload or post material. As a result, social media platforms, blog owners and video- and photo sharing services are frequently also referred to as hosts. Social media platforms or 'web 2.0. applications' are intermediaries that allow third parties to post

[6] Edwards, L. The Fall and Rise of Intermediary Liability Online. In Edwards, L. & Waelde, C. (eds) Law and the Internet. 3rd edn. Portland: Hart Publishing 2009, p. 47

[7] The Economic and Social Role of Internet Intermediaries, OECD April 2010, p. 9, www.oecd.org/internet/ieconomy/44949023.pdf (11.02.2016)

information and materials, and encourage individuals to connect with other users and share content. Finally, search engines are software programmes that use algorithms to retrieve data from a database or network in response to a query, and index and present the information as a series of hyperlinks on a webpage. These four categories of intermediaries can in turn be distinguished from content providers or publishers, meaning those online actors that are responsible for producing the information in the first place and distributing it online.[8]

Although it is important to differentiate between the different categories of internet intermediaries since they may be subject to contrasting liability regimes, this has become increasingly difficult as they often tend to play more than one role.[9] For example, Google is most known for its search engine, but it also provides the social media platform Google+ and the blog-publishing service Blogger. Furthermore, Google is also an ISP through its super-high-speed landline internet service, Google Fiber and a wireless carrier through Google Fi.[10]

The multiple roles played by internet intermediaries is not, however, the only source of confusion when it comes to determining their definition. When referring to internet actors that fulfil the functions of intermediaries, authors of legislative texts and academic literature have not limited themselves only to the term intermediary. Different EU documents alone use several distinct phrases in addition to intermediary[11], such as information society service providers[12], intermediary service providers[13], online platforms[14], providers of electronic communications services[15], and internet access services[16]. Moreover, the e-Commerce Directive in turn makes a distinction between three types of intermediary service providers, namely mere conduits, caching and hosting

[8] Internet intermediaries: Dilemma of Liability, Article 19, p 6, www.article19.org/data/files/Intermediaries_ENGLISH.pdf (10.02.2016)
[9] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.10
[10] Cade Metz, „How Google's New Wireless Service Will Change the Internet", WIRED Magazine, 03.03.2015, www.wired.com/2015/03/googles-new-wireless-service-will-change-internet/ (05.03.2016)
[11] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 195, 02.06.2004 p 0016 - 0025
[12] e-Commerce Directive
[13] Ibid
[14] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe {SWD(2015) 100 final}, COM(2015) 192 final, Brussels, 6.5.2015, eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=EN (14.01.2016)
[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201 , 31.07.2002 p 0037 - 0047
[16] European Commission Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM(2013) 627 final 2013/0309 (COD)

providers[17]. Finally, intermediaries are also differentiated on the basis of whether they can be considered as active or passive.[18]

Since the e-Commerce Directive is often described as the cornerstone of the EU's legal framework for online services, the terms and definitions in the directive require closer examination. The overall aim of the directive is ensuring the free movement of information society services between the EU member states.[19] Such services are defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service".[20] Despite the fact that the directive does not offer any interpretation of the term intermediary service providers, the definition of information society services implies that the liability regime in the directive covers, in addition to the traditional ISP sector, also a wider extent of actors who sell goods and services online, offer online search tools and the so-called 'pure' telecommunications, cable and mobile communications companies that offer access to networks. The phrase "at the individual request of the recipient", however, indicates that television and radio broadcasters do not fall within the remit of the limited liability regime.[21] Also, although a service may be free to the recipient, this does not mean that the provider of that service is automatically excluded from the scope of the ECD if the service forms part of an economic activity.[22] Considering that the limited liability regime in the ECD is devised to benefit rather than burden intermediaries, the term intermediary service providers should be interpreted widely since one of the prevalent business models in the industry is giving away major products or services for free and then generating revenue out of them in indirect ways, such as associated advertising.[23]

Since the e-Commerce Directive was enacted in 2000, the internet and its actors have significantly changed, and therefore it does not necessarily cover some of the newer activities of internet actors that are now regarded as types of intermediaries, like for example search engines or the providers of hyperlinks, or some participative web platforms.[24] As a result, the European Commission has

[17] Articles 12-14 ECD
[18] Joint Dissenting Opinion of Judges Sajó and Tsotsoria in *Delfi AS v Estonia* (Application no. 64569/09, ECtHR Grand Chamber 16 June 2015). C-324/09 *L'Oreal SA v eBay International AG* (2011).
[19] Art 1(1) ECD
[20] Article 2(a) of the ECD refers back to the definition in Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal L 217, 05/08/98 P. 0018 - 0026
[21] Edwards, L. (2009), *supra nota 6*, p.62
[22] Recital 18 of the ECD
[23] Edwards, L. (2009), supra nota 6, p.63
[24] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.11

come up with a new umbrella term for actors such as search engines, online market places, video sharing platforms, payment systems, social networks and news aggregators. They are now all covered by the term online platform, which is defined as an "undertaking operating in two (or multi)-sided markets, which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least one of the groups". The definition goes on to explain that certain online platforms can also qualify as intermediary service providers, but mere internet access providers are explicitly excluded from its scope.[25] It has been suggested that the reasoning behind the Commission's new definition is to justify a limitation of the scope of the liability exemptions in the e-Commerce Directive, especially Article 14 which refers to hosting providers.[26]

Finally, intermediaries are also classified as either active or passive. When the e-Commerce Directive was adopted, internet intermediaries were largely of a passive nature and only transmitted or stored material on behalf of their users.[27] Thus, the liability exemptions in the directive are only applicable when the activity of an intermediary service providers is of a "mere technical, automatic and passive nature".[28] In the present day, however, intermediaries have become increasingly active. Although the content is still created by the users, the role of the internet intermediary is not anymore limited to merely transmitting, storing or publishing the material on behalf of the user, but instead they perform an active role in the organisation and functioning of the platforms.[29] This distinction was also recently employed by Judges Sajó and Tsotsoria in their dissenting opinion in the *Delfi* case. The judges characterised active internet intermediaries as hosts who provide their own content and also open their intermediary services to allow for third parties to comment on that content.[30] The judges explicitly stated that an active intermediary is not the same as a publisher or editor, since the publication of comments on a

[25] European Commission public consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights: Intermediaries, Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud

[26] Sophie Stalla-Bourdillon, Internet intermediaries: How are you? What do you do? What the European Commission has to say (14.09.2015), available at https://peepbeep.wordpress.com/2015/09/14/internet-intermediaries-how-are-you-what-do-you-do-what-the-european-commission-has-to-say/ (01.02.2016)

[27] Bart van der Sloot, Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe, 6 (2015) JIPITEC 211, para.3

[28] Recital 42 ECD

[29] Van der Sloot (2015), *supra nota 26*, para. 3

[30] Joint Dissenting Opinion of Judges Sajó and Tsotsoria in *Delfi AS v Estonia* (Application no. 64569/09, ECtHR Grand Chamber 16 June 2015), at para. 1

platform provided by an active intermediary occurs without the prior decision or permission of that intermediary.[31]

Therefore, due to the multitude of varied definitions and interpretations of what exactly an internet intermediary is, a broad construction of the term shall be used. The main focus in the present thesis is on internet intermediaries, which facilitate internet-based communications by allowing persons to upload or post their own content on a platform provided by the intermediary. Such intermediaries will be referred to interchangeably as intermediaries, hosting providers or intermediary service providers. Moreover, when discussing specific legal instruments, such as the e-Commerce Directive, the specific terminology used in that particular instrument will be used.

### 1.2. History of Intermediary Liability

Internet intermediaries are often seen as the obvious points of control for online content due to their position as gatekeepers or actual enablers of internet communications. As gatekeepers they are in a place where they can eliminate access to objectionable content and also to identify infringers.[32] The liability of internet intermediaries for content generated by third parties is one of the earliest legal issues that concerned the emerging internet industry in the beginning of the 1990's. The initial cases, which mainly originated in the United States, focused on the liability of the first ISP's such as AOL and CompuServe for hosting, transmitting or publishing material that was libellous, defamatory or contained pornographic material.[33] These early cases resulted in widely diverging regimes both across different legal systems as well as within the same system due to diverse classifications of authorship, responsibility, control and different types of content.[34]

Around the same time, the issue of liability for content became a major concern not just for the traditional ISPs, but also for a wider range of internet hosts, such as universities, traditional media organisations going digital, software providers, libraries and archives, chatrooms, blog sites,

[31] Ibid, paras. 30-32
[32] Jonathan Zittrain, *A History of Online Gatekeeping*, Harvard Journal of Law and Technology, Vol. 19, No. 2, 2006, p.253-298, at 254
[33] OECD Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy '*The Role of Internet Intermediaries in Advancing Public Policy Objectives – Forging partnerships for advancing policy objectives for the Internet economy, Part II'* DSTI/ICCP(2010)11/FINAL 22 June 2012, p.10
[34] Ibid

individuals creating personal web pages and the emerging social media sites. Moreover, potential liability affected not only traditional telecommunications companies, but also internet backbone providers, cable companies and mobile phone communications providers since they started providing content and value-added services like geolocation data.[35] This all evidenced the need for a liability regime for internet intermediaries that was practical, consistent, acceptable to the internet industry and also protective of consumers, individuals, institutions and businesses.[36]

Therefore, as the emerging industry sector of internet intermediaries became aware of their possible high-risk status for liability for content authored by third parties in the mid-1990's, they called for a form of special statutory regimes and pleaded a case for immunity, which rested on the following three factors: first, that they lacked effective or actual control over the user-generated content; second, that it was inequitable to impose liability upon a mere intermediary; and third, that liability could have potentially negative consequences on growth, innovation and the public interest.[37]

### 1.2.1. Lack of Effective Legal or Actual Control

Internet intermediaries strongly argued that it was in practice impossible for them to check the legality of all the material that passed through their networks or servers without huge amounts of delays and expenses, and moreover, it was not practicable or even legal for them to do so without violating their users' privacy and confidentiality. Automated filtering technologies and classification of information was offered as a possible measure to circumvent the issue, but in the late 1990's such technologies tended to radically under- and over block. Furthermore, with regard to topics such as libel, false advertising and hate speech, where semantic meaning is extremely dependant on the nuances of human interpretation, blocking was, and still is, regarded as completely impractical.[38]

However, despite the questions about the effectiveness and proportionality of filtering from the technical, cost and operational viewpoints, some still argue that these are easy to sidestep.[39] The

[35] Edwards, L. (2009), *supra nota 6*, p.49
[36] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.10
[37] Edwards, L. (2009), *supra nota 6*, pp. 58-59
[38] Ibid, p.59
[39] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.11

potential feasibility of automated filtering is evidenced by the *LICRA v Yahoo!*[40] case of 2000 before the Superior Court of Paris. The case was brought by LICRA (League Against Racism and Anti-Semitism) against Yahoo in France arguing that the ease with which French users could access the auction pages on the Yahoo US website where they could find Nazi memorabilia for sale was a clear violation of French criminal law.[41] Yahoo did not dispute that the offer of such goods for sale violated French law but they contended, inter alia, that they could not be held liable because the Yahoo France regional site did not contain any Nazi or Third Reich items for sale.[42] Importantly, Yahoo also argued that it was impossible for them to determine the national identity of people visiting their auction pages, meaning that an order forbidding access to pages containing Nazi goods for all persons from France would in practice have the effect of requiring Yahoo to remove the violating material from its site in entirety.[43]

In response, the French court passed the issue to a technical sub-committee for investigation, which reported that Yahoo was in fact in a position to identify and block access to 90% of French citizens as evidenced by their use of such measures for serving advertisements in the relevant language to users from whatever country of origin. The country of origin of around 70% of users could be identified from IP addresses and the rest of the 20% could be established by asking users to fill in a form declaring their country of origin.[44] The committee also acknowledged that for those users, who accessed the site through portals that guaranteed their anonymity, Yahoo would have more difficulty in exercising control over what pages they could visit, but ultimately held that control could still be exercised by limiting access to only those surfers who disclosed their geographical origin. Accordingly, the Court held that the issues faced by Yahoo do not constitute insurmountable obstacles and that Yahoo must prohibit users from France from viewing those pages that violate the French Criminal Code by offering Nazi items for sale.[45]

The *LICRA v Yahoo!* decision was considered unusual on the ground that it concerned location-based blocking instead of content-based blocking since the third parties, who posted items for sale on Yahoo, manually classified the types of items. In cases of pure automated content classification,

[40] *Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France (LICRA) et UEJF c. Yahoo! Inc. et Société Yahoo! France* (20 November 2000, Tribunal de Grande Instance de Paris, Superior Court of Paris).
[41] Marc H. Greenberg, *A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market*, 18 Berkeley Tech. L.J. (2003) pp. 1191-1258, at 1206
[42] Greenberg (2003), *supra nota 40*, p. 1207
[43] Ibid, p. 1209
[44] Edwards, L. (2009), *supra nota 5*, p.59-60
[45] Greenberg (2003), *supra nota 40*, p. 1210

the most prevalent view was that Internet intermediaries could not yet successfully automate the filtering of unwanted or unlawful material and also stay in business. In addition, ISPs and hosts were subject to a risk as a result of content authored by parties with whom they in most cases did not have a contractual relationship.[46]

### 1.2.2. Inequity of Imposing Liability upon a Mere Intermediary

The second argument was based on the notion that Internet intermediaries are nothing more than messengers or mere conduits instead of content providers. Accordingly, they should not be treated as creators or publishers of the material but as conduits such as the postal service and phone companies that, for example in the United States, are not liable for any content facilitated by them and are also obliged to respect confidentiality.[47] Even though it can be debated that the business model for, at least a consumer ISP, has always been partly dependent on users storing material which might possibly be illegal, in practice, a perception of so-called common enterprise between the internet intermediary and the user was not apparent at that stage of industry development. Arguments against this lack of perception of the internet intermediary industry as culpable collaborators were only made by the music industry at the time, since their business model was already under threat from online piracy.[48]

### 1.2.3. Potential Negative Consequences of Liability on Growth, Innovation and the Public Interest

The growth and innovation of the internet economy are dependent on a reliable and developing internet infrastructure and imposing the burden of full liability on internet intermediaries would arguably discourage them from investing in improvements and research, which in turn would have an adverse effect on access and the quality of their services. In addition, it was thought at the time that such stringent regulation would encourage the industry to move outside of Europe and the United States. Therefore, giving internet intermediaries immunity, or at least creating a limited liability regime for content authored by third parties, would be in the public interest.[49] Otherwise

[46] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.12
[47] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.12
[48] Edwards, L. (2009), *supra nota 5*, p.60-61
[49] Ibid, p.61

access to the information society by the public would be seriously impeded.[50] These concerns are still present today in the context of a wider debate on the issue of maintaining respect for legal standards in the online environment.[51]

The above concerns played a major role in the development of the limited liability regimes both in the United States with regard to the Digital Millennium Copyright Act and in Europe with respect to the e-Commerce Directive.[52]

### 1.3. Adoption of Limited Liability Regimes in the United States and Europe

In the United States, by 1995, the online industry began to recognise the severe threat posed by the threat of intermediary liability for content created by third parties. This risk is illustrated by the *Stratton Oakmont, Inc. v Prodigy Services Co.*[53] case, which suggested that service providers who took an editorial role with regard to their users' content were publishers, and therefore responsible for their users libel and other torts. The case partly served as a catalyst for the US Congress enacting Section 230 of the Communications Decency Act (CDA) 1996, which prohibits treating service providers as the publishers or speakers of any information that is provided by others.[54] Section 230 is often considered to have contributed to the remarkable growth over the past 15 years of online websites and services, particularly sites enabling user-generated content.[55]

In addition to the CDA, the Digital Millennium Copyright Act (DMCA) 1998 established a limited liability regime in the form of 'safe harbours' with regard to infringements of intellectual property rights. The DMCA makes a distinction between four categories of service providers that escape liability under certain conditions: access providers or mere conduits that offer access to networks and transmission through these networks, caching providers that temporarily store material on their servers, hosting providers that store information or host webpages, and search engine providers that offer links to websites and make content searchable.[56] The DMCA also instituted an additional

[50] Ibid, p.85
[51] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.11
[52] Edwards, L. (2009), *supra nota 6*, p.58-59
[53] 1995 WL 323710 (N.Y. Sup. Ct. 1995)
[54] 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material, https://www.law.cornell.edu/uscode/text/47/230 (01.02.2016)
[55] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.10
[56] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998), para. 512, https://www.law.cornell.edu/uscode/text/17/512 (01.02.2016)

immunity condition, which obliges intermediaries to expeditiously remove illegal material upon notification.[57]

In Europe, on the other hand, the European Commission challenged the claim for limited liability of internet intermediaries because of the role that intermediaries could potentially play in controlling and fighting online pornography, libel, hate speech, spam and other forms of objectionable content. The reasons behind this were not only obvious policy goals such as child protection, but also a more general desire to increase public trust and confidence in the internet as a safe space for economic activity.[58] Furthermore, the debate in Europe around the intermediary liability regime was not simply tied to different types of content, like libel, pornography or copyright infringement, but also to a more comprehensive problem of whether intermediaries should be held accountable for content that they made available to the public and also, whether they could act in a particular way to manage the responsibility and thus limit their liability.[59] On the other hand, there were also concerns that if intermediaries were held to be liable for user-generated content on analogous grounds as publishers, it could restrict service providers from entering the market.[60]

Therefore, by 2000, a relative consensus had emerged both in Europe and the United States that a balance had to be struck. While it was recognised that different types of internet service providers perform different functions and require specific responses, they should in principle be guaranteed an exemption, or at least a limited exemption, from liability for content created by third parties.[61] It was agreed that the liability exemptions should commonly consist of two basic principles: immunity for intermediaries for third party content if they do not modify the content nor are aware of its illegal character, and no general obligation to monitor content.[62] In order for intermediaries to benefit from immunity, they should be prepared to remove or block access to illegal or infringing content when required.[63] In the EU, these principles were enshrined in the e-Commerce Directive 2000/31, which is the main topic of the following chapter.

[57] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p. 14
[58] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p. 12
[59] Ibid, p.11
[60] OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives, *supra nota 32*, p. 12
[61] Edwards, L. (2009), *supra nota 5*, p.61
[62] OECD, The Economic and Social Role of Internet Intermediaries, *supra nota 6*, p.6
[63] Ibid, p.12

Presently, the most common intermediary liability issues concern hosting and transmission of child pornography and other forms of criminal content, violations of intellectual property rights, especially copyright, and libellous or defamatory material. The prevalence of music, film and information content piracy and peer-to-peer networks has, in addition to the detrimental impact on authors and distributors, exposed internet service providers and hosts to unseen amounts of potential risk, and thus piracy concerns continue to change this area of law.[64]

[64] Ibid, p.11

## 2. The Regime under the e-Commerce Directive

In 2012 activities of internet intermediaries in the EU contributed around €430 billion to the GDP of the EU, comprising of a direct GDP contribution of €220 billion and a more long-term indirect GDP contribution of €210 billion resulting from the productivity impact of intermediaries on other companies.[65] Thus, in addition to their influential role as facilitators of communication, intermediaries are also a key driver of economic growth. Recognising the potential for this, by the year 2000 a consensus had emerged that intermediary service providers should not be held liable for content created by third parties on the condition that they agreed to cooperate with the authorities when asked to remove or block access to any illegal content. This consensus was reflected in Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market[66] (the e-Commerce Directive or ECD), which is considered to be the cornerstone of the EU's legal framework for online services.

### 2.1. Intermediary Liability Provisions in the e-Commerce Directive

Without the limited liability regime of the e-Commerce Directive, online intermediaries would be prone to monitoring as well as censoring their users' information or terminating their online services altogether just to be able to avoid being held liable or having an injunction imposed on them.[67] The drafters of the ECD recognised this and clarified that the free movement of information society services can in many circumstances be a specific reflection of a more general principle of EU law, namely freedom of expression, and therefore the directives that govern the supply of such services must guarantee that the right can be freely exercised.[68] The main goal of the directive is to support the proper functioning of the internal market of the EU by guaranteeing the free movement of information society services between the EU member states[69] while also providing legal certainty and ensuring consumer confidence in electronic commerce[70]. In addition

[65] Copenhagen Economics. Study on the impact of online intermediaries on the EU economy. April 2013, p. 8 https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/6/226/0/The%20impact%20of%20online%20intermediaries%20-%20April%202013.pdf (06.03.2016)
[66] 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, OJ L 178, 17.07.2000, p 0001-0016
[67] Van Eecke (2011), *supra nota* 3, p. 1456
[68] Recital 9 ECD
[69] Art 1(1) ECD
[70] Recital 2 ECD

to the liability protection of intermediaries, the ECD also created a freedom of service provision principle and harmonised numerous transparency requirements as well as online contracting procedures.[71]

The relevant part of the e-Commerce Directive for the purposes of the present thesis is Section 4, consisting of Articles 12 to 15, which outline a harmonised regime of the liability exemptions for intermediary service providers throughout the EU. The Section 4 regime includes three types of activities – mere conduit, caching and hosting, and contains two types of protection – against liability and monitoring obligations.[72] Accordingly, Articles 12-14 safeguard certain intermediaries against complaints about the transport or storage of information supplied or requested by their users, and Article 15 protects against injunctions and orders requiring them to actively monitor or search their platforms for illegal content.[73] The three types of activities are related to each other and an intermediary can practice all of them at the same time.[74] The exemptions from liability are only applicable in cases where the activity of the intermediary service providers is of a "mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge nor control over the information which is transmitted or stored".[75] Unlike, for example, the US DMCA which focuses on one single area of law, the ECD deals with all kinds of content, like for example intellectual property rights, criminal obscenity, defamation, libel, etc.[76]

The first of the three types of activities that are exempt from liability are the so-called 'mere conduits' i.e. intermediaries that act as a go-between transmitting content originating from one party and destined for another, such as service providers that provide access to the internet. According to Article 12 ECD, in order to qualify for immunity from liability under the provision, the intermediary must not initiate the transmission, select the receiver of the transmission nor modify the information being transmitted.[77] Mere conduits typically comprise of either network access services or network transmission services that transmit great amounts of data at the request of their subscribers and are commonly provided by traditional internet access providers and

[71] Van Eecke (2011), *supra nota* 3, p. 1457
[72] Ibid, p. 1462
[73] Van Eecke (2011), *supra nota* 3, p. 1462
[74] Mlynar, V. A Storm in ISP Safe Harbour Provisions: The Shift from Requiring Passive-Reactive to Active-Preventative Behaviour and Back (2014) 19 Intell. Prop. L. Bull. 1, p.3
[75] Recital 42 ECD
[76] Edwards, L. (2009), *supra nota 5*, p.64
[77] Art 12(1) ECD

infrastructure operators.[78] This kind of an approach is in accordance with the laws governing neutral carriers like the post and telephone companies.

Article 13 ECD covers caching i.e. when an intermediary makes local copies of remote websites when requested in order to make the delivery of those pages faster on subsequent requests.[79] Common examples of intermediaries that engage in caching are proxy servers that store local copies of webpages to speed up the consequent consultation of the page by other users.[80] For example, if a user situated in San Francisco wishes to access a website stored on servers that are located in Prague, and intermediary may cache the content of the Czech website, that is, make a copy on its servers based in the United States. Consequently, users' requests do not have to go back and forth between San Francisco and Prague every time they want to access the Prague website.[81] Such intermediaries avoid liability as long as they do not modify the information, comply with conditions on access to the information, update the cached copy regularly according to industry practice and remove cached copies or disable access to the information upon obtaining actual knowledge that the initial source of the information has been removed or access to it has been disabled or the removal or blocking of access has been ordered by a court or administrative authority.[82] As caching effectively makes transmission of information more efficient, and thus the web faster, it is important that it is not legally encumbered.

Article 14 ECD deals with intermediaries that host or store more than temporary content authored by third parties. An example of a service covered under the provision is a webhosting company that provides space on the web to its customers where they can upload content that can be published on a website.[83] Article 14 differentiates between levels of knowledge, depending on what kind of a claim is made against the intermediary. Thus, hosting intermediaries are exempt from criminal liability if they lack actual knowledge of illegal activity or information, and immune from civil liability if they have no such actual knowledge and they are not aware of facts or circumstances from which the illegal activity or information is discernible.[84] Furthermore, intermediaries must expeditiously remove or block access to the illegal information once they become aware of its

[78] Van Eecke (2011), *supra nota* 3, p. 1457
[79] Edwards, L. (2009), *supra nota 6*, p.64
[80] Van Eecke (2011), *supra nota* 3, p. 1462
[81] Mlynar (2014), *supra nota 70*, p.3
[82] Art 13(1) ECD
[83] Van Eecke (2011), *supra nota* 3, p. 1463
[84] Art 14(1)(a) ECD

infringing nature.[85] Compared to Articles 12 and 13, under which an intermediary can benefit from the exemption of liability only when the intermediary is passive, meaning not in any way involved with the information that is being transmitted, hosting providers can still benefit from the liability exemption on the condition that their involvement does not lead to them having actual knowledge or awareness of illegal information.[86]

The final provision of Section 4, Article 15, prohibits EU Member States from imposing a general obligation on mere conduits, caching or hosting providers to monitor the information they transmit or store, or to actively seek cases indicating illegal activity. Regardless of this prohibition, courts and administrative authorities can, however, impose injunctions on intermediaries requiring them to terminate or prevent infringements.[87] Furthermore, the prohibition of monitoring obligations only applies to those of a general nature, since monitoring requirements in individual cases that are specific and clearly defined are allowed.[88] This is evidenced by the *Scarlet v Sabam* case, which concerned the former's refusal to establish a filtering system in order to prevent copyright infringements.[89] The CJEU ruled that the preventive monitoring required by the envisaged filtering system would, in effect, oblige the intermediary to actively monitor all the data relating to all its customers, which is prohibited under Article 15(1) of the ECD.[90] Therefore, the injunction imposed by the Belgian Court was held to be incompatible with the ECD.

Member States are also allowed to oblige intermediaries, who host content authored by third parties, to apply duties of care that can reasonably be expected from them and that are specified by domestic law with the aim of detecting and preventing particular illegal activities.[91] The ECD itself does not specify what exactly such duties of care should entail, but arguably, they should only concern public and criminal law and not private law as otherwise the point of Article 15 in the context of the directive's hosting provisions would be contradicted.[92] Article 15(1) is considered to complement Article 14 in the sense that if intermediary service providers were

[85] Art 14(1)(b) ECD
[86] Recital 43 ECD
[87] Articles 12(3), 13(2) and 14(3) and Recital 45 ECD
[88] Recital 47 ECD
[89] CJEU. Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, [2010] ECR I-11959
[90] Ibid, para 40
[91] Recital 48 ECD
[92] Edwards, L. (2009), *supra nota 5*, p.65

required to actively monitor their networks on a continuous basis, then they would automatically have to be aware of any illegal content, thus not qualifying for the protection of Article 14.[93] Further, Article 15(2) creates to additional requirements that Member States have the discretion to decide whether to impose on information society service providers. Firstly, the Member States may require that the service providers inform national authorities about any purported illegal activities of their users, and secondly, Member States may oblige providers to disclose the identity of users with whom they have storage agreements. The latter was discussed by the CJEU in the *Promusicae* case, which concerned a preliminary ruling questioning whether Member States were required to establish such a requirement to achieve more effective copyright protection and whether such a requirement could potentially violate the right to respect for private life of the users.[94] The Court held that Member States are not required to lay down an obligation to communicate personal data to ensure effective copyright protection.[95] The CJEU also explained that in transposing directives into domestic legal system a fair balance needs to be struck between the different fundamental rights protected by the EU legal order, in this case the right to protection of property and the right to effective remedy on the one hand, and the right to the protection of personal data on the other.[96] However, the CJEU did not provide any further guidelines on how the balance between the competing rights should be achieved.

As a final point, it should also be mentioned that if an intermediary does not qualify for any of the exceptions set out above, this does not automatically mean that the intermediary is subject to a liability as such. As a consequence, the intermediary cannot benefit from the immunity under the e-Commerce Directive, but the issue of liability will go on to be determined under the applicable national law for the specific type of infringing content.[97]

[93] Van Eecke (2011), *supra nota* 3, p. 1465
[94] CJEU. Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-00271
[95] Ibid, para. 58
[96] Ibid, para. 68
[97] Van Eecke P., Truyens M., Legal analysis of a Single Market for the Information Society, New rules for a new age? A study commissioned by the European Commission's Information Society and Media Directorate-General, November 2009. Chapter 6: Liability of Online Intermediaries, p.10. http://ec.europa.eu/information_society/newsroom/cf/document.cfm?doc_id=842 (08.12.2015)

## 2.2. Interpretation Issues in the e-Commerce Directive

Even though the objective of the EU legislature in enacting the ECD was to ensure uniform treatment of intermediaries as unengaged middlemen, who should not be required to police their users' content, the significantly diverging implementations of the Directive and decisions from national courts of the Member States as well as the Court of Justice of the EU (CJEU) illustrate that this has not always been the case. With regard to user-generated content, Article 14 has turned out to be by far the most contentious provision of the ECD[98] due to the numerous different interpretations of the key concepts of the provision. This section will examine these concepts in the light of the case law of the CJEU as well as a few notable decisions of the national courts of the EU.

### 2.2.1. Illegal Activity or Information

In order to benefit from the limited liability regime in Article 14(1), a hosting provider is required to take down illegal information upon obtaining actual knowledge or awareness of it. This indicates that hosting providers will have to make an assessment of what exactly constitutes as illegal information in order to decide whether to block or remove it. However, encumbering intermediaries with the task of evaluating the legitimacy of a complaint regarding infringing content is thought to be ill-advised and even unfair since private companies may not have enough legal knowledge to determine the potential illegality of third party content, especially when the content in question is not manifestly illegal, as may occur if the subjective rights of individuals are at stake.[99] An example of such a situation is, for example, the instance where Google was pressured to remove an offensive anti-Muslim video from YouTube. Although Google refused to comply with the US Government's request contending that no policies were infringed, they did decide to block access to the video from countries in the Middle East.[100] This was considered by many as a disproportionate response which resulted in accusations of paternalism and moral policing of free expression by Google.[101] Moreover, the requirement that intermediaries must determine whether

[98] Edwards, L. (2009), *supra nota 5*, p.65
[99] Kuczerawy, A. Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative. Computer Law & Security Review 31 (2015) 46-56, p. 48
[100] Eva Galperin, *Why Google Shouldn't Have Censored The Anti-Islamic Video* (Sep 17, 2012) http://techcrunch.com/2012/09/17/why-google-shouldnt-have-censored-the-anti-islamic-video/ (01.03.2016)
[101] BBC News, *YouTube under new pressure over anti-Muslim film* (19 September 2012) http://www.bbc.com/news/technology-19648808 (01.03.2016)

the content authored by their users is illegal also seems to be at odds with the notion put forward in Directive 2009/136, namely that it is a task for the Member States, and not the service providers, to determine what constitute as lawful or harmful content, applications, or services.[102]
First of all, the national laws of most Member States require that hosting providers only take down obviously or manifestly illegal information. For example, under Austrian law the violation must be obvious to a non-lawyer without additional investigation so that it would be easily noticeable for the hosting provider, while under French and Dutch law the infringement must be manifestly illicit.[103] A similar standard was outlined by the CJEU in the *L'Oreal v eBay* case, where the judges referred to illegal information as "facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question".[104] The use of the phrase diligent economic operator instead of a specialised auction provider, which eBay is, indicates the high level of the threshold as the information must be obviously illegal to any attentive economic operator, not just highly specialised hosting providers.[105]

Secondly, most information is not illegal as such and its potential illegal nature depends on its use. However, in order to be able to determine the use, the hosting provider requires additional knowledge, which in practice they do not have access to. For instance, a digital copy of a movie may at the same time be legal for one user and illegal for another, contingent on whether the user needed to, and did, acquire a license. In addition, the copyright exceptions in a particular state, such as the right to quote, parody and educational use should also be considered.[106] Therefore, in a lot of cases, it is nearly impossible to determine, at least at first sight, whether the particular content in question is or is not illegal.

Thirdly, the assessment of illegality frequently requires considerable legal knowledge, which technically oriented online service providers usually lack. What is more, even for trained lawyers and specialists, interpreting existing rules and regulations is complicated due to the ever changing interpretations and definitions of the key concepts in the e-Commerce Directive by domestic as

[102] Recital 31, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337/11, 18.12.2009 p 0011-0036
[103] Van Eecke (2011), *supra nota* 3, p. 1467
[104] CJEU. Case C-324/09, *L'Oréal SA and Others v eBay International AG and Others* [2011] ECR I-06011, para 120
[105] Van Eecke (2011), *supra nota* 3, p. 1467
[106] Ibid, p. 1466

well as EU courts.[107] Lastly, the e-Commerce Directive does not protect hosting providers against claims from its users for unlawfully removing content after being notified by a third party.[108] According to the Directive, the removal or blocking of material must be carried out in compliance with the principle of freedom of expression, as well as with the procedures governing the matter under national law.[109] This is in direct contrast with the US DMCA, which explicitly protects the hosting provider from liability in cases where the service provider has in good faith disabled access to or removed content claimed to be illegal, even if it turns out not to be infringing.[110]

Consequently, in attempting to determine whether certain content should be removed or blocked, hosting providers come across serious problems when trying to assess which member states' laws apply, whether the material is illegal and whether the material is illegal enough for it to warrant removal. For example, a court in Austria held that trademark infringements could not be classified as being obviously illegal, while German courts have held them to be obvious infringements.[111] Moreover, on the topic of defamation, a Dutch court held that content was not manifestly unlawful, while an Austrian court stated that defamatory and insulting statements could be characterised as obvious, as everyone is capable of determining the libellous nature of such statements.[112]

### 2.2.2. Actual Knowledge

As previously mentioned, Article 14(1)(a) ECD established two different levels of knowledge. In order to rely on the exemption from criminal liability, the hosting provider cannot have actual knowledge of illegal activity or information, and to be protected from civil liability, hosts cannot be aware of facts or circumstances from which the unlawful activity or information is apparent. The rationale behind the provision is to create a clear defence for hosting providers unless the required level of knowledge can be established.[113] It is not, however, completely clear what exactly

[107] Van Eecke (2011), *supra nota* 3, pp. 1466-1467
[108] Ibid, p. 1467
[109] Recital 46 ECD
[110] DMCA s. 512(g)(1)
[111] Verbiest, Spindler, Riccio and Van der Perre, Study on liability of Internet intermediaries (study prepared for the European Commission - Markt/2006/09/E Service Contract ETD/2006/IM/E2/69) 12 Nov. 2007, p.38 http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (14.03.2016)
[112] Van Eecke (2011), *supra nota* 3, p. 1468
[113] McCarthy, H.J. Is The Writing on the Wall for Online Service Providers? Liability For Hosting Defamatory User-Generated Content Under European and Irish Law. 14 Hibernian L.J. 16 2015, 16 – 55, p. 28

the term 'actual knowledge' means or where the border between these categories of knowledge lies.

The interpretations in EU Member States vary significantly from each other. For instance, in Spain, only notifications from competent authorities, such as courts, are sufficient to supply actual knowledge. This has resulted in a situation under Spanish law that even if a provider is well aware that it is hosting illegal content, it will still be considered as lacking actual knowledge.[114] Courts in other Member States, like for example Germany and Austria, indicate to general legal standards of obtaining knowledge of infringing content, while countries such as Finland relate actual knowledge to a formal notice and take-down procedure, albeit restricting this only to copyright violations. When it comes to other content, Finland applies more common legal standards.[115] Furthermore, some Member States, like Latvia and Hungary, do not even provide a distinction between actual knowledge and awareness of facts and circumstances in relation to civil or criminal liability.[116]

Furthermore, the question also arises whether the term actual knowledge implies actual human knowledge or whether computer knowledge, such as a software filter searching for and finding illegal information, is also sufficient. Once again, the national courts of EU Member States have not provided a uniform answer and neither has the CJEU supplied any specific guidance on the matter. However, based on the *L'Oreal v eBay* judgment it can be assumed that the CJEU does require human knowledge, since the examples provided by the court all refer to human actions.[117]

Another significant issue that arises in the context of actual knowledge is whether a hosting provider must also take down future infringing material that is similar or identical to a current violation, because the service provider can be presumed to have sufficient knowledge after being notified once concerning a particular infringement.[118] In his Opinion in the *L'Oreal v eBay* case, Advocate General Jääskinen explicitly excludes future infringements by stating that legally knowledge can only refer to the past and/or the present.[119] Moreover, the Advocate General (AG) goes on to mention that the requirement of actual knowledge excludes construed knowledge, and

[114] Peguera, M. "I just know that I (actually) know nothing": actual knowledge and other problems in ISP liability case law in Spain. E.I.P.R. 2008, 30(7), 280-285, p. 280
[115] Study on intermediary liability, *supra nota 106*, p.28
[116] Ibid, p.30
[117] Van Eecke (2011), *supra nota* 3, p. 1475. Also L'Oreal v eBay, para. 122
[118] Van Eecke (2011), *supra nota* 3, p. 1476
[119] AG Jääskinen Opinion in *L'Oreal v eBay*, para 162 (ECLI:EU:C:2010:757)

therefore it is not enough that the hosting provider should have known or had good reasons to suspect infringing activities.[120] According to the AG, actual knowledge means knowledge of past or present information, activity or facts that the intermediary service provider has as a result of an external notification or its own voluntary research.[121]

The CJEU, however, did not clarify in their decision whether knowledge of a current infringement would necessitate the hosting provider to impede similar violations in the future, as they merely listed characteristics which measures imposed on hosting providers must satisfy.[122] These include the measures having to be effective and dissuasive, fair, proportionate and not unreasonably costly, and they must not create barriers to legitimate trade and must not amount to active monitoring of all of their customers data.[123] Nevertheless, with regard to an injunction requiring the prevention of future infringements, all these conditions will likely be met simultaneously in only the rarest of circumstances. The CJEU's decision seems to reflect the idea that the e-Commerce Directive implies that a rightholder must notify a hosting provider regarding the specific details of every illegal item, since otherwise a hosting provider cannot be presumed to have actual knowledge or awareness of the infringing nature of particular content.[124]

### 2.2.3. Lack of a Harmonised Notice and Take-Down Procedure

Although hosting service providers are immune from liability if they lack knowledge of infringing activity or content, they retain that immunity only if they act expeditiously to remove or disable access to that information upon receiving knowledge of its illegality. The e-Commerce Directive does not expressly provide a notice and take-down procedure (NTD), but implies it through its requirements for liability exemptions.[125] Under this procedure, victims of infringement, such as copyright owners, can bring offending material to the attention of a hosting intermediary and request the expeditious removal or blocking of access to the allegedly infringing content.[126] Although the US DMCA, which the ECD was based on, sets out detailed rules specifying the conditions for the notice and take-down procedure, when the e-Commerce Directive was adopted,

[120] Ibid, para 163
[121] Ibid, 164
[122] Van Eecke (2011), *supra nota* 3, p. 1478
[123] *L'Oreal v eBay (*2011), *supra nota 97*, paras. 136-140
[124] Van Eecke (2011), *supra nota* 3, p. 1478
[125] Kuczerawy (2015), *supra nota 92*, p. 48
[126] Articles 14(1)(b) ECD

it was decided that such a procedure should not be regulated in the directive itself.[127] It was instead hoped that industry self-regulation in the field would establish notice procedures for different types of content.[128] Therefore, the ECD merely limits itself to a suggestion that Member States establish procedures regulating the removal or disabling of access to content.[129] Self-regulation, however, has proved to be extremely ineffective as in most EU Member States no procedures were introduced, thus resulting in a lack of adequate safeguards in many jurisdictions.[130] This has resulted in inconsistent notice and take-down procedures across the EU, and occasionally even within the territory of a single state. This creates considerable legal uncertainty for internet intermediaries as well as conflicts with the objective of guaranteeing the free movement of information society services between the EU Member States.[131]

Most EU Member States have not set up formal notice and take-down procedures, leaving it up to the national courts to decide how an intermediary should be informed and what level of detail the notification has to contain. One exception to the rule is France, where a precise procedure is established in Article 6-I 5° of the French e-Commerce Act (LCEN).[132] Accordingly, an intermediary is considered to be aware of the infringing material when they are notified of the following elements: the date of the notice, the identifying details of the notifying natural person or legal entity, the description of the litigious facts and their exact location, the reasons specifying why the content must be removed that include the appropriate legal provisions, copy of the correspondence sent to the author or editor of the infringing material or activities requesting their removal or modification, or evidence that the author or editor could not be contacted. The reasoning behind the detailed nature of the provision is the importance of providing intermediaries with the means allowing them to meet their obligation to act rapidly as failure to do so has been often strictly punished in cases where content has been removed after more than a few days.[133]

Other exceptions include Spain, where a competent body, such as a court or an administrative authority must require the removal or disabling of infringing material, and Italy, where a notice is

[127] Article 16 and Recital 40 ECD. Also Verbiest et al (2007), *supra nota 104*, p.5
[128] Walzel, S. European Commission Consults on Notice and Takedown (24.08.2012) http://blogs.lse.ac.uk/mediapolicyproject/2012/08/24/european-commission-consults-on-notice-and-takedown/ (10.02.2016)
[129] Art 14(3) ECD
[130] Kuczerawy (2015), *supra nota 92*, p. 49
[131] Mlynar (2014), *supra nota 70*, p.4
[132] Law no. 2004-575 of 21 June 2004 on Confidence in the Digital Economy
[133] Christine Gateau and Christelle Coslin, *No 'Stay Down' Obligation for Hosting Providers in France*, published on 02/07/2013, available at http://www.scl.org/site.aspx?i=ed32661, accessed on 2 March 2016

also required from the relevant authorities although it remains unclear whether intermediaries should inform their users about the notification. Likewise, Finland and Hungary have detailed formal procedures in place, but only for infringements relating to intellectual property rights and Lithuania has selected optional notification procedures.[134] In Member States that lack any formal procedures, some criteria have emerged from their case law and legal doctrine. For example, in Germany the notice must include details as to the claimed copyright in order to be sufficient. In addition, some Member States, like Belgium and the Netherlands, have adopted codes of conduct that clarify how intermediaries should deal with take-down requests.[135] Interestingly, the CJEU has had very little to say on the matter. In its decision in the *L'Oreal v eBay* case the Court stated that notifications of allegedly illegal activities or information must be sufficiently precise and adequately substantiated.[136] The CJEU, however, failed to clarify what constitutes as a sufficiently precise and adequately substantiated notice.

Another issue with regard to the notice and take-down procedure concerns the meaning of the term 'expeditiously' in Article 14(1)(b). According to these provisions, an intermediary will avoid liability if it expeditiously removes or disables access to information that they host, but there is no guidance given in the Directive as to what it exactly means and whether it allows time to, for example, investigate facts, consult a lawyer or seek an official opinion.[137] Also, in practice, there is disagreement between stakeholders on whether the EU legislature should define the meaning of expeditiously since it has been understood differently by various stakeholders.[138] The rightholders argue that the term should be clearly defined and the time period short, while intermediaries claim that leaving the meaning of the term unspecified will provide them with some flexibility in applying it.[139]

Requiring intermediaries to promptly decide to either remove or block content in order to benefit from the liability exemption basically makes them a judge in their own cause as the notice and take-down procedure implies that intermediaries experience a conflict of interest. In such a

[134] Van Eecke (2011), *supra nota* 3, p. 1485
[135] Ibid, pp. 1484-1485
[136] CJEU. Case C-324/09 *L'Oréal SA and others v eBay International AG and others*, para. 122
[137] Reed, C. Policies for Internet Immunity. 2009 Computers and Law, Vol. 19(6), 20
[138] European Commission, Online Services, Including e-Commerce in Single Market, Commission Staff Working Paper, 11.1. 2012 SEC(2011) 1641 final; Accompanying the document: Communication from the Commission to the European Parliament, the Council The European Economic and Social Committee and the Committee of the Regions, A Coherent framework to boost confidence in the Digital Single Market of e-Commerce and other online services, COM(2011) 942, p.37-39
[139] Kuczerawy (2015), *supra nota 92*, p. 51

situation, the safest option is to act upon any evidence of illegality, no matter how negligible, without engaging in an analysis of the specific circumstances and balancing the different rights that require protection. This can, in turn, bring about preventive over-blocking of legitimate content.[140] This is illustrated by a case in the UK, where an online childcare forum was forced to settle a claim of defamation for comments made by its users on a site bulletin board as they were uncertain whether the removal of comments within 24 hours constituted expeditious removal.[141] This is an extremely short time period and does not take into account the type of content nor the size of the organisation. In large intermediary service providers it may take a while for a take-down request to reach the right person, or for the location of the particular infringing content to be located on a large website, while in small intermediaries it can be complicated to identify who is responsible for evaluating take-down requests, especially if it is a non-profit making or volunteer organisation. Moreover, it seems that once notice of infringing content has been given and the expedient time period has expired, liability is strict, regardless of whether there are technical or administrative difficulties with the take-down.[142]

Furthermore, since material is in most cases removed without hearing from the party whose content it is being deleted, therefore preventing that party from providing evidence of the legality of the information, this could lead to private censorship.[143] It also opens up a possibility for abuse by fictitious victims, for example by business competitors or even political adversaries.[144] When a private party, and a potential defendant, determines arbitrarily whether content should be removed or access to it disabled can lead to a conflict with the right to freedom of expression, as set out in Article 10 of the ECHR[145] and Article 11 of the EU Charter[146]. This is in direct contrast to Recital 46 of the ECD, which expressly specifies that the removal or disabling of access should be carried out in observance of the right to freedom of expression.

### 2.2.4. Neutral Role of Hosting Providers

[140] Kuczerawy (2015), *supra nota 92*, p. 48
[141] OUT-LAW, 'Mumsnet settles with Gina Ford but queries libel law' http://www.out-law.com/page-8040 (25.02.16)
[142] Edwards, L. (2009), *supra nota 5*, p.66
[143] Rosa Julià-Barceló and Kamiel J. Koelman, *Intermediary Liability In The e-Commerce Directive: So Far So Good, But It's Not Enough*, Computer Law & Security Review, 16 (2004) 4, 231–239, at 235
[144] Verbiest et al (2007), *supra nota 104*, p.15
[145] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms
[146] Charter of Fundamental Rights of the European Union

According to Van Eecke, the supposed neutral role of hosting providers is a common misunderstanding in both case law and legal doctrine when interpreting the e-Commerce Directive and it has generated considerable legal uncertainty for hosting providers. The source of this misconception is Recital 42 of the ECD, which states that the liability exemptions in the directive only apply in cases where the intermediary's activity is of a "mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge nor control over the information which is transmitted or stored". The wording of the recital gives the sense that it concerns all of the three categories of intermediaries covered in the directive, while on closer examination it refers to terms such as "access to a communication network", "information is transmitted or temporarily stored" and "making transmission more efficient", which point only to mere conduits and caching providers.[147]

The CJEU has also adopted this misconceived position in its case law. In the *Google France v Louis Vuitton* case the court held that in order to determine whether an intermediary qualifies for the exemption under Article 14 ECD, "it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores".[148] Nonetheless, in the Court's opinion, it is the domestic courts who are in the best position to decide whether the role played by Google qualifies as neutral.[149] In his opinion in the *L'Oreal v eBay* case, AG Jääskinen, on the other hand, contested the idea that neutrality is the right test for determining the applicability of the liability exemption in Article 14.[150] The AG favoured the approach of focusing on the intention of the ECD to create exemptions for specific types of activity exercised by a service provider instead of attempting to determine whether the intermediary was neutral or not, since hosting intermediaries will almost always have some amount of involvement with their users.[151]

The CJEU, however, did not explicitly follow the AG's opinion and considered that an operator of an online marketplace does not qualify for the liability exemption only in circumstances when the operator takes an active role, which presumes knowledge or control of the data stored.[152] Nonetheless, the differences between the AG's opinion and the Court's decision are actually rather

[147] Van Eecke (2011), *supra nota* 3, p. 1482
[148] CJEU. Joined cases C-236/08 to C-238/08, *Google France SARL v Louis Vuitton Malletier SA; Google France SARL v Viaticum SA et al; Google France SARL v CNRRH SARL et al* [2010] ECR I-02417, para 114
[149] Ibid, para 119
[150] Advocate General Jääskinen, Opinion on the case Case C-324/09 *L'Oreal v eBay* para. 146.
[151] Ibid, para 149
[152] *L'Oreal v eBay (2011), supra nota 97*, para. 123

minimal as the CJEU interpreted neutrality as a lack of knowledge, which results in the hosting provider being protected from liability when offering tools for its users to upload, categorise, display or search for content.[153]

### 2.3. Intermediary Liability for Hosting User-Generated Defamatory Content

Although, as evidenced above, most CJEU case law interpreting the provisions of Section 4 of the ECD involve cases concerning violations of intellectual property rights, the provisions have also been applied in defamation and libel claims. The main question in such cases has been whether an intermediary should be considered a publisher or a hosting provider when it comes to defamatory content created by the users of intermediaries. When the e-Commerce Directive was drafted there was a clear distinction between an online hosting service provider and a content provider or publisher. Nowadays, however, it is nearly impossible to make such a distinction due to the growth and success of websites such as Facebook, YouTube, Google Plus, eBay, etc., whose success essentially relies on UGC since the platform derives revenue from encouraging its users to use the sites to publish and share their own content. The use of the websites is free for the users and the platform's income comes from the sale of some form of advertising.[154] In this context, the question arises under what circumstances an internet intermediary can be held liable as a publisher of material that has been created and published by third parties.

This was the subject of the *Papasavvas* case, where the CJEU considered the Article 14 hosting exception in the context of online defamation. In the case, an online newspaper operator hosted defamatory content authored by its employees and freelance journalists engaged by it. Unsurprisingly, the CJEU held that the online newspaper could not claim exemption from civil liability since it could not be considered an intermediary service provider within the meaning of Section 4 of the ECD. The decision was based on the fact that a newspaper publishing company has, in principle, knowledge about the information which it posts and it also exercises control over that information.[155] The decision is straightforward in the sense that employees of an online newspaper cannot be considered to be the users of the service, but have to be held as the publishers.

---

[153] Van Eecke (2011), *supra nota* 3, p. 1483
[154] Edwards, L. (2009), *supra nota 5*, p. 67
[155] CJEU. Case C-291/13, *Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd and Others* [2014] ECLI:EU:C:2209, para 45

Therefore, it was entirely reasonable to not extend the exemption in Article 14 to the online newspaper operator.

The distinction between hosting providers and publishers has also often been used by national courts of the EU Member States to avoid applying the immunity provisions of the ECD. For instance, French courts have held both MySpace and Dailymotion (a French YouTube equivalent) liable for infringements for content posted on their websites by their users. With regard to MySpace, it was considered to be a publisher since it generates profits from the advertisements on its website, and therefore it could not benefit from the hosting exemption in the ECD.[156] In contrast, although the French court found that Dailymotion was not a publisher even though it sells advertising space, it was still held liable for deliberately providing its users with the means of publishing illegal material on its website.[157] These decisions show how the fact that an intermediary simply provides the platform and makes revenue from it is often found to be enough for holding an intermediary liable as a publisher. Notably, however, the Dailymotion decision was later overturned by the French Supreme Court based on an insufficient notice of the infringement.[158]

The courts in the United Kingdom have also on several occasions been called to address the question of intermediary liability for user-generated defamatory content. The *Imran Karim v Newsquest Media*[159] case concerned a libel action focusing on defamatory user comments relating to an article posted on bulletin boards that were hosted on the same webpage as the article. While the article itself was not defamatory, the hosting provider nevertheless removed both the article and the user comments immediately after receiving a complaint.[160] On these facts, the court ruled that the intermediary service provider could successfully invoke Regulation 19, which transposes Article 14 of ECD in to English law, on the grounds that the service provider did not possess actual knowledge of the unlawful activity until notified, and upon notice it expeditiously removed the defamatory comments. Interestingly, the court was able to reach such an outcome by severing the article from the user comments posted on the bulletin boards.[161]

---

[156] Edwards, L. (2
009), *supra nota 5*, p.72
[157] Ibid
[158] Jondet, N. France: EC Directive 2000/31 of 8 June 2000 on certain legal aspects of information society services, in particular electronic cfommerce, in the internal market, art.14; Act on Confidence in the Digital Environment of 21 June 2004, art.6-I-2 and 5 - "Nord-Ouest v Dailymotion". IIC 2012, 43(5), 614-617
[159] *Imran Karim v Newsquest Media Group Ltd* [2009] EWHC 3205 (QB)
[160] McCarthy, H.J. (2015) *supra nota 113,* p. 25
[161] Ibid, p. 26

The principle of severance established in the *Imran Karim* decision was also endorsed in the *Kaschke v Hilton*[162] ruling. The case concerned the question whether a website operator hosting political blogs could invoke Regulation 19 in a defamation case where the intermediary service provider had edited parts of the website, but not the defamatory article that was hosted somewhere else on the website. The court concluded that the service provider could rely on Article 19 noting that it was permissible to invoke the hosting exemption even in circumstances where the provider was not entirely passive in its hosting activities, but only because it did not edit the defamatory content and it was hosted elsewhere on the site.[163] Thus, *Kaschke* seems to indicate that the hosting defence will not be available for defamatory content hosted on the homepage in a situation where that page has been significantly moderated by the hosting provider.[164] This illustrates the notion that hosting providers need to be very careful when undertaking voluntary monitoring and moderating with respect to UGC since such conduct can cost them their immunity under Article 14 of the ECD. Moreover, as will be discussed below, the precedent established by these decisions is the complete opposite of the recent *Delfi AS v Estonia* saga, where a news portal did not qualify as a hosting provider within the meaning of Article 14.

Despite the *Imran Karim* and *Kaschke* decisions, the UK courts, however, also seem to move in the direction of increased responsibility for hosting service providers. The Court of Appeal in *Tamiz v Google*[165] was called to address the question whether Google could be held liable as a publisher for defamatory comments hosted on its Blogger service. The court held that Google's role was not purely passive, since it makes the notice board available to bloggers on its own terms and can easily remove or disable access to any notice that does not abide by those terms.[166] Therefore, the Court held Google liable for the defamatory comments posted by its users due to a five week delay in removing the defamatory comments from its platform.[167] However, it is important to distinguish that following the *Tamiz* judgment, websites which host user-generated content are still effectively immune from liability for defamatory content posted by their users provided they do not in some way participate in the initial publication of such content. The liability

[162] *Kaschke v Hilton* [2010] EWHC 690 (QB)
[163] Ibid, para 52
[164] McCarthy, H.J. (2015) *supra nota 113,* p. 27
[165] *Tamiz v Google* [2013] EWCA Civ 68 (QB)
[166] Ibid, para 33
[167] Ibid, para 34

arises only after a complaint is made and the intermediary fails to remove the unlawful content.[168] This approach is in line with the notice and take-down regime of the e-Commerce Directive.

[168] Griffiths, R. Normality restored: website hosts may again be liable for defamatory user generated content (19 February 2013) http://www.fieldfisher.com/publications/2013/02/normality-restored-website-hosts-may-again-be-liable-for-defamatory-user-generated-content#sthash.N3zfDajq.dpbs (11.11.2015)

## 3. Protection of Personal Data

Every single day two and a half quintillion bytes of data is created and the development of the internet has resulted in an environment in which this data can be accessed ubiquitously.[169] Data has even been described as "the pollution problem of the information age" with privacy protection being the environmental challenge".[170] Moreover, personal data is considered to be the oil of the digital economy and thus the hottest commodity on the market today.[171] It is this personal data that is the subject matter of data protection laws. Data protection is an area of law that handles the ways in which individuals and organisations may and should treat people's personal information.[172] It concerns informational privacy, that is, the right to control what is known about you. Although the kind of information protected is defined differently in various countries, it generally includes personal data, such as name, address, date of birth, contact details, financial, medical and social work details, identifiable photos, political views, sexual, genetic, biometric, racial and ethnic details, school records, etc.[173]

In the EU, the distribution of user-generated content that includes third parties' personal data may involve infringements of data protection rights if it does not comply with the conditions established under the data protection laws, such as for example, the consent of the data subject. Such infringements are aggravated by the sheer size of the internet and the fact that once data has been distributed online, it is basically impossible for the data subjects to exercise any control over their personal data. On the other hand, the publication of content that contains third parties' personal data may also involve the exercise of fundamental rights, such as freedom of expression and information. Such cases comprise of the so-called peer violations of privacy interests since they concern violations of individuals' data protection rights by other, similarly positioned, individuals.[174]

---

[169] Buttarelli, G. Data protection as a bulwark for digital democracy. Keynote speech at the 6th International e-Democracy 2015 Conference on Citizen rights in the world of the new computing paradigms. 10 December 2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-12-10_eDemocracy_EN.pdf (14.01.2016)

[170] Schneier, B. Data and Goliath's Big Idea. 6 March 2015. https://www.schneier.com/blog/archives/2015/03/data_and_goliat_3.html (14.01.2016)

[171] Mikkonen, T. Perceptions of controllers on EU data protection reform: A Finnish perspective. C.L.S.R. 30 (2014) 190-195, at 190

[172] Carey, P. Data Protection: A Practical Guide to UK and EU Law. 3rd edn (Oxford OUP 2009) p.1

[173] Edwards, L. Privacy and Data Protection Online: The Laws Don't Work. In Edwards, L. & Waelde, C. (eds) Law and the Internet. 3rd edn. Portland: Hart Publishing 2009, p.445

[174] Azevedo Cunha, M. V., Marin, L. & Sartor, G. Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web (2012) International Data Privacy Law, Vol. 2, No. 2, pp. 50-67, at 52

The aforementioned violations are very different from what are considered to be typical interferences in privacy and data protection, which involve disproportionate relationships between state authorities or big organisations on the one hand, and individuals on the other.[175] Therefore, the online publication of user-generated content that contains a third party's personal data creates a conflict between the user posting the information and the data subject, whose personal information is published. As a result, a conflict arises between the user's freedom of expression and the data subject's rights to privacy and data protection. However, the conflict also involves the intermediary that provides the platform where the content is disclosed and distributed.[176] This chapter aims to examine the cases and circumstances where intermediary service providers may be held liable for violations of third parties' data protection rights conducted by their users through their networks and platforms.

### 3.1. Overview of Data Protection Legislation

The origins of informational privacy lie in the combination of fear for individual privacy during and after World War II, and the increase of widespread automated data processing. As the world rebuilt itself in the 1940s and 1950s, the pressing fear in the Western world of a total surveillance state that had been seen in Nazi Germany and the Soviet Union, and the growing use of computers in the 1970s led to the adoption of data protection legislation. Thus, the German state of Hesse enacted the first data protection act in 1970, with several other German states following shortly thereafter, and the earliest national legislation aimed at the protection of individuals' personal data processed in computers was adopted in 1973 in Sweden. The first international legal instrument governing the issue of data protection, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), was adopted by the Council of Europe (CoE) in 1981.[177] Convention 108, in turn, led to the adoption of the Data Protection Directive.

While in the United States privacy questions regarding the processing of personal data in the private sector are predominantly dealt with a self-regulatory and market-based approaches, in the

[175] Ibid
[176] Azevedo Cunha, M. V., Marin, L. & Sartor, G., at 65
[177] Edwards (2009), Privacy and Data Protection Online, *supra nota 160*, p.447

European Union, on the other hand, personal data is a matter of fundamental human rights, directives and ordinary legislation.[178] The right to the protection of personal data is explicitly provided for in Article 8 of the Charter of Fundamental Rights of the European Union (EUCFR or the Charter), which came into force on 1 December 2009. Secondary EU law relating to the topic, however, was adopted already in 1995 in the form of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[179] (DPD or the Data Protection Directive). It is worth noting at the outset that the DPD does not make any specific reference to the right to data protection, although the CJEU has recently held that the provisions of the directive should be interpreted in the light of the fundamental rights outlined in the Charter, namely the Article 7 right to respect for private life and the Article 8 right to the protection of personal data.[180] The Data Protection Directive does, however, specifically refer to the right to privacy with respect to the processing of personal data.[181] Finally, the right to respect for private and family life is also enshrined in Article 8 of the CoE's Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

In the context of these legal instruments, a question arises regarding the exact difference between the right to privacy and the right to data protection, and the simple answer is that the relationship between these two rights is not altogether clear. The fact that the EU Charter has included data protection as a separate right, makes it different from other international human rights instruments and there seems to be no uniform answer to the question whether data protection is a subcategory of the right to privacy, or whether it should be treated as a self-standing right.[182] Despite the reality of the CJEU constantly conflating these two rights, analysis of the protection offered by them has shown that although they are heavily overlapping, data protection offers individuals enhanced control over their personal data.[183] There are two main distinctions with respect to the range of data falling within the scope of both rights: unlike the notion of privacy interference, the concept of personal data is not context-dependent, and personal data includes data relating to unidentified yet identifiable individuals.[184] Moreover, data protection rules are also arguably more effective at

[178] Azevedo Cunha, Marin & Sartor, supra nota 2, at 53
[179] 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, OJ L 281, 23.11.1995, p 0031-0050
[180] CJEU. Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [ECLI:EU:C:2014:317], para 68
[181] Article 1, Directive 95/46/EC
[182] Lynskey, O. Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order. I.C.L.Q. 2014, 63(3), 569-597, at 573
[183] Lynskey, at 582
[184] Lynskey, at 583

minimising the risk for individuals in relation to tangible risks caused by data processing, such as identity theft.[185] For example, Article 17 of the DPD requires data controllers to implement appropriate technological and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

Data protection laws were created with the intention of protecting the privacy of individual citizens against the state, and therefore, unlike with the right to privacy, legal persons, such as companies and similar unincorporated associations are not protected under these laws.[186] Thus, the aim of the DPD is to "protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data" and to ensure the "free flow of personal data between the Member States" for reasons connected with the protection offered to individuals.[187] The DPD applies to personal data, defined as information relating to an identified or identifiable natural person.[188] Only information pertaining to facts about an individual can be considered as personal data, thus for example, a person's address is personal data, but an analysis of his domicile for legal purposes is not.[189] Accordingly, the aim of the definition of personal data is to differentiate identifying information from anonymous information, and not to distinguish between several categories of information based on the extent to which the information may pertain to the privacy interests of the data subject.[190] Nevertheless, the exact scope of personal data differs from one EU Member State to another due to a degree of discretion that national legislators have exercised in implementing the DPD into their domestic laws. For example, in Portugal, information concerning deceased people is considered as personal data, while in the United Kingdom it is not. The CJEU has through in their case law somewhat constrained the differences in national approaches. For instance, in the *Scarlet v SABAM* decision they held that IP addresses are protected personal data since they allow for users to be precisely identified.[191] The Data Protection Directive also distinguishes between two technology-neutral roles that have particular responsibilities under the directive: the data controller and the data processor.[192] According to

[185] Lynskey, at 589
[186] CJEU. Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paras 52-53
[187] Article 1, the DPD
[188] Art 2(a), the DPD
[189] CJEU. Opinion of AG Sharpston in Joined Cases C-141/12 and C-372/12 *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M, S* [ECLI:EU:C:2014:2081], para 56
[190] Tracol, X. Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it. Computer Law & Security Review 31 (2015) 112-119, at 116
[191] Azevedo Cunha, Marin & Sartor, *supra nota 2*, at 53
[192] Varadi, S., Kertesz, A. and Parkin, M., The necessity of legally compliant data management in European cloud architectures. C.L.S.R. 28 (2012) 577-586, at 579

Article 2(d) of DPD, a data controller is the natural or legal person which determines the means of the processing of personal data, whereas a data processor is a natural or legal person which processes data on behalf of the controller (Article 2(e) of DPD).

### 3.2. Internet Intermediaries – Data Controllers or Data Processors?

Whenever something is done with personal data, whether it is collecting, storing, adapting, publishing, blocking or deleting data, it almost always falls within the definition of data processing.[193] Accordingly, ISP's that provide access to the internet, a telecommunications or electronic mail service with the sole purpose of transmission of data are considered as data processors, while the person from whom the message containing personal data originates will be the controller. However, the ISPs will usually be regarded as controllers with respect to the processing of any additional personal data required for the operation of the service.[194] Therefore, ISPs should be regarded as controllers only with respect to traffic and billing data, and not for personal data that is transmitted.[195] Likewise, a hosting provider is also, in principle, a processor for any personal data distributed online by its users, who use the service for their website hosting and maintenance. In case the hosting provider, however, further processes data contained on the websites for its own purposes, then the host will become a controller with respect to that particular processing.[196] It is also worth noting that collecting and making available personal data that has already been published in the media, even in an unaltered form, still constitutes as processing of personal data covered by the directive.[197]

It has been argued that the fact that the issues concerning the protection of personal data are explicitly excluded from the scope of the e-Commerce Directive[198] could lead to the conclusion that a hosting intermediary would be responsible for violations of third parties' data protection rights committed by their users even in situations where the intermediary has engaged in neutral

[193] Art 2(b), the DPD
[194] Recital 47 DPD
[195] Article 29 Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". WP 169, 00264/10/EN. Adopted on 16 February 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (02.03.2016), p. 11
[196] Article 29 Working Party. Opinion 1/2010 on the concepts of "controller" and "processor". Page 25
[197] CJEU. Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831, para 49
[198] Article 1(5)(b) and Recital 14 ECD

activities.[199] On the other hand, however, the above interpretation of the Data Protection Directive, namely that hosting providers will be considered as data processors and not controllers with respect to personal data disclosed by their users, seems to be consistent with the intermediary liability regime in the e-Commerce Directive. In both cases, as long as a hosting provider deals with content on behalf and according to the instructions of the user of its service, the intermediary remains protected from liability.

The *Google Spain* case, better known as the 'right to be forgotten' ruling, is the first in which the CJEU has been called upon to interpret the DPD in the context of internet search engines.[200] The ruling seems to indicate that even though an intermediary service provider might be able to qualify for a liability exemption under the e-Commerce Directive, in similar circumstances, it would still be subject to the extensive responsibilities under the Data Protection Directive. The applicant in the case, Mr Costeja Gonzáles, had various social security debts resulting in his house being put up for action and, as required by Spanish law, a notice of the auction was published in a Spanish newspaper. When the newspaper archives were digitalised and put online, two links to the auction notice appeared in response to a Google search of his name. Since the information in the article was not illegal, the newspaper could not be required to remove it. Therefore, the question arose whether Google should be required to remove the link to the article from its search engine results and whether it could be held liable for the processing of personal data.[201] The Court stated that the activities of the search engine, consisting of finding the information published on the internet by third parties, indexing and storing it automatically and making it available to internet users according to a certain order of preference indicate that it is the search engine which determines the purposes and means of the processing of personal data. Therefore, Google was held to be a data controller pursuant to the meaning of Article 2(d) of the DPD.[202] Furthermore, the Court distinguished search engines from publishers of websites, saying that the former's activities with regard to the processing of personal data are additional to those carried out by the latter.[203]

The decision in *Google Spain* can be contrasted with an earlier decision of the CJEU, namely the *Google France v Louis Vuitton* judgment, where the Court examined whether a referencing service

[199] Azevedo Cunha, Marin & Sartor, at 57
[200] CJEU. Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*
[201] Ibid, *Google Spain SL,* paras. 14-18
[202] *Google Spain*, paras. 33 & 41
[203] *Google Spain*, para. 35

provider could benefit from the liability exemption in Article 14 of the e-Commerce Directive. The Court based their answer on evaluating the question of neutrality[204] and stated that the facts that the referencing service had to be paid for, or that the payment terms were determined by Google, or that Google provided general information to its customers, would not in themselves result in depriving Google of the exemption.[205] The CJEU held that Article 14 ECD must be interpreted to mean that the liability exemption therein applies to an internet referencing service provider in circumstances where the service provider has not played an active role as to give it knowledge of, or control over, the data stored.[206] Even though the final decision on the neutrality of the referencing service provider was left to the national courts, the decision demonstrates that under the e-Commerce Directive, a search engine could, under certain conditions, qualify for a liability exemption, while under the Data Protection Directive it would in any case be considered a data controller.

Finally, the regime under Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the e-Privacy Directive), also needs to be briefly evaluated. The e-Privacy Directive governs the processing of personal data by providers of publicly available electronic communications services[207] and aims to complement the Data Protection Directive and, unlike the latter, extends protection to legal as well as natural persons.[208] Therefore, passive intermediaries, such as ISPs that provide access to the internet, are subject to a number of obligations. For instance, they must ensure the security of their networks[209] and process personal data confidentially and may not put on or pull information from a computer, for example, by using cookies, without the consent of the user[210]. In relation to these data processing activities, it is the service providers who are liable for the processing.[211]

[204] Cornthwaite, J. To key or not to key? The judgment of the European Court of Justice in the Google France Adwords cases. E.I.P.R. 2010, 32(7), 352-359, at 356
[205] Google France, para 116
[206] CJEU. Joined cases C-236/08 to C-238/08, *Google France SARL v Louis Vuitton Malletier SA; Google France SARL v Viaticum SA et al; Google France SARL v CNRRH SARL et al* [2010] ECR I-02417, para 120
[207] Article 3(1), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002 p 0037-0047
[208] Art 1(2) e-Privacy Directive
[209] Art 4 e-Privacy Directive
[210] Art 5 e-Privacy Directive
[211] Van der Sloot (2015), *supra nota 26*, para 18

### 3.3. Exemptions from Liability under the Data Protection Directive

The Data Protection Directive does not apply to the processing of personal data undertaken in the course of an activity which is outside the scope of EU law, including processing operations involving public and state security, defence and activities of the state in areas of criminal law, and by an individual in the course of a purely personal or household activity.[212]

#### 3.3.1. The Purely Personal or Household Activity Exemption

The purely personal or household activity exception was the subject of the CJEU's judgment in the *Lindqvist* case, which concerned a woman who had identified and included personal information, including health data, about her fellow church volunteers on her web site.[213] First off, the Court held that the act of referring, on a website, to individuals and identifying them by name and other means, constitutes processing of personal data within the meaning of Article 3(1) of the DPD.[214] Secondly, the Court clarified that circumstances, where the processing of personal data consisting of publication on the internet, which in turn results in those data being made available to an unlimited number of people, are not encompassed by the personal or household exemption, since it only covers activities that are carried out in the course of private or family life of individuals.[215] Therefore, uploading content on the internet without limiting its accessibility will preclude the application of the exception.[216] However, it is possible that the exemption could apply to webpages that are only accessible with a password or to private social media profiles with a limited number of users, although the exact line between private and public must be ascertained on a case-by-case basis.[217]

Whereas the CJEU, when assessing the personal and household exemption in *Lindqvist,* relied on the assumption that if something happens online, it is automatically accessed by an indefinite number people and, as a result, it must be public, the Article 29 Working Party (Art 29 WP) more

[212] Article 3(2) of the DPD
[213] CJEU. Case C-101/01 *Bodil Lindqvist v v Åklagarkammaren i Jönköping* [2003] ECR I-12971
[214] Ibid, para 27
[215] Ibid, para 47
[216] Warso, Z. There's more to it than data protection – Fundamental rights, privacy and the personal/household exemption in the digital age. Computer Law and Security Review 29 (2013) 491-500, at 493
[217] Van der Sloot, B. Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe, 6 (2015) JIPITEC 211, para 21

recently in their opinion on social networking extended the application of the exemption to some online activities.[218] The Art 29 WP stated that many social media users operate within a wholly personal sphere, communicating with people as part of their personal, family or household relations, and in such cases the household exemption applies, while the rules governing data controllers do not.[219] However, having a high number of third party contacts, providing access to a profile to all users of the social network, or allowing the data to be indexable by search engines all indicate that the household exception does not apply and the user would be considered a data controller. Thus, the same legal regime would apply as when a person uses other technology platforms to publish data on the internet.[220] The Art 29 WP also stressed the need to limit the application of the household exemption in order to protect the rights of third parties, especially with regard to sensitive personal data and explained that even if the exemption applies, a user could still be liable under general provisions of domestic law, such as defamation.[221]

### 3.3.2. The Journalistic Exemption

In addition to the purely personal and household activity exception, the Member States are also required to adopt, in their national laws, exemptions or derogations for the processing of personal data carried out solely for journalistic purposes or for the purpose of artistic or literary expression, provided they are necessary to reconcile the right to privacy with rules regulating freedom of expression.[222] The CJEU held in the *Satamedia* case that the journalistic exemption does not only apply to media undertakings but to all persons engaged in journalism.[223] Further, the fact that the publication of data is done with the aim of making a profit does not mean that it is not an activity solely for journalistic purposes, since it is natural that an undertaking seeks to generate a profit from its activities.[224] Likewise, the medium which is used for transmitting the processed data, whether conventional such as a paper, or electronic, such as the internet, is not determinative as to whether an activity falls within the exemption.[225]

---

[218] Warso, Z. (2013), *supra nota 201*, at 495
[219] Article 29 Working Party. Opinion 5/2009 on Online Social Networking. WP 163, 01189/09/EN. Adopted on 12 June 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (02.03.2016), p. 3
[220] Opinion 5/2009 on Online Social Networking, p. 6
[221] Opinion 5/2009 on Online Social Networking, p. 7
[222] Art 9 DPD
[223] CJEU. C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831, para 58
[224] Ibid, para 59
[225] Ibid, para 60

Overall, the CJEU took the view that the notion of journalism must be interpreted broadly to encompass all activities whose object is the disclosure of the information, opinions or ideas to the public.[226] The aforementioned interpretation seems to indicate that modern media and active intermediaries using UGC and amateur journalists and bloggers may also potentially invoke the journalistic exception.[227] The broad interpretation of the journalistic exception does not, however, extend to search engines. The CJEU held in the *Google Spain* case that although a publisher of a web page consisting in the publication of a third party's personal data could benefit from the journalistic exemption in Article 9 of the DPD, the same could not be said for an operator of a search engine.[228] Thus, even though active internet intermediaries will usually be considered as data controllers with regard to the processing of personal data, they cannot rely on the journalistic exemption unless they are the editor of the published information.[229]

### 3.4. Data Protection Legislation as a Tool for Reputation Management

In recent years, it seems that the market for the so-called reputation management services has suddenly waken up to the power of data protection legislation after years of being ignored as an internet take-down tool in favour of more appealing causes of action, such as libel and the right to privacy.[230] The catalyst for this sudden change was the *Google Spain* judgment, which made lawyers and other professionals providing reputation management services realise that publishing text on the internet is equal to data processing. Further, any person who can exercise control over such processing can be categorised as a data controller, provided that person falls within the rather wide scope of the EU and domestic data protection rules by virtue of having some kind of a physical presence in the relevant jurisdiction.[231] This in turn means that the person must comply with all the required data protection principles of the DPD, which include transparency, purpose specification and limitation, erasure of data, confidentiality, availability, integrity and indemnification.[232]

---

[226] Ibid, para 61
[227] Van der Sloot (2015), *supra nota 26*, para 22
[228] *Google Spain*, para. 85
[229] Van der Sloot (2015), *supra nota 26*, para. 23
[230] Hurst, A. Data privacy and intermediary liability: striking a balance between privacy, reputation, innovation and freedom of expression. Ent. L.R. 2015, 26(6), 187-195, at 187
[231] Ibid
[232] Art 6 DPD

Thus, data protection becomes somewhat more straightforward and also much easier to rely on compared to privacy and defamation laws. There is no need for long debates and arguments over the exact meaning of terms like "reasonable expectation of privacy", "public domain", "serious harm" and so on, especially in cases where the data that is being processed is simply inaccurate instead of out of date or insignificant.[233] This has resulted in a potential short cut for individuals who are being defamed online inasmuch as they can now ensure that a particular defamatory article is more difficult to find by asking Google or any other search engine to remove links to the article from their search results. This is much easier in practice than sending a take-down request to the website operator, and although the article could still be found by searching the website directly, it is still an effective remedy as nowadays most content online is found through search engines.[234]

In the aftermath of the *Google Spain* judgement, some recent cases in the UK have drawn attention to a conflict between data protection law on the one hand, and defamation, privacy and copyright laws on the other. Namely, the nature of the relationship between the remedies that are available under data protection law and the safe harbour defences under the e-Commerce Directive is extremely unclear. Therefore the question under what circumstances an internet intermediary may be liable in damages for the publication of unlawful content that it facilitates and what steps it can be obliged to take by way of injunction to prevent such publication needs to be examined more closely.[235] Under English law, in order for a claimant to establish liability against an internet intermediary, it must show that the intermediary is a common law publisher and not a mere conduit within the meaning of the ECD.[236] For example, in *Metropolitan Schools v Google* it was held that Google's functions as a search engine are passive in nature and accordingly it was considered to be a mere conduit and not a common law publisher.[237] This is similar to the *Tamiz v Google*[238] judgment, where it was held that while Google was not a common law publisher at the time of publication, it could become one when it receives notice of any unlawful material. This was the case in the Northern Irish case of *CG v Facebook Ireland* where the court found Facebook liable

[233] Hurst, *supra nota 230*, at 187
[234] Hurst, *supra nota 230*at 188
[235] Hurst, *supra nota 230*at 188
[236] Section 10, Defamation Act 2013 (UK)
http://www.legislation.gov.uk/ukpga/2013/26/pdfs/ukpga_20130026_en.pdf (10.03.2016)
[237] *Metropolitan International Schools Ltd (t/a SkillsTrain and t/a Train2Game) v Designtechnica Corp (t/a Digital Trends)* [2009] EWHC 1765 (QB), para 80
[238] Supra nota 159

in damages for privacy violations because it failed to remove a page after being notified that it contained abusive information about a convicted sex offender.[239]

The above examples show that the defences in Section 4 of the ECD are applicable to cases covering defamation and the right to privacy. However, according to Recital 14 of the ECD, they do not apply to data protection claims. This could result in a situation where, regardless of a notice to an intermediary, if the unlawful data processing by the intermediary is sufficient to cause the data subject damage, the subject can claim damages from the intermediary unless the intermediary can prove that it is not responsible for the event causing the damage.[240] Under English law, since the *Vidal-Hall v Google Inc* judgment, damage also includes non-financial loss.[241] Considering that Article 23 of the DPD does not specifically require the data controller to have actual knowledge of the unlawful data processing, a situation where a data controller failed to adopt satisfactory security measures to prevent a hacker from publishing unlawful personal data would most likely result in the data controller being held liable notwithstanding its actual awareness of the unlawful nature of the data.[242]

The inconsistencies between defamation and privacy laws on the hand, and data protection on the other also apply to the question what steps an intermediary can be required to take to remove unlawful content from its platforms. The removal of content is usually required by way of blocking injunctions, which are most often used in intellectual property cases. In the *L'Oreal v eBay* case, the CJEU held that such injunctions can be granted to prevent both existing and future infringements on the condition that they are "effective, proportionate and dissuasive".[243] Moreover, a court, when granting a blocking injunction, must take care not to impose on internet intermediaries a general monitoring obligation contrary to Article 15 of the ECD. However, the next question that comes up is whether these conditions on blocking injunctions also apply to intermediaries who are data controllers. In the *Mosley v Google Inc* case, where Google asked the court to strike out an individual's case under the English Data Protection Act 1998, which sought to require Google to block access to photos of the individual engaging in private sexual activity, the court favoured the approach that the DPD and the ECD should be read in harmony.[244]

[239] *CG v Facebook Ireland Ltd* [2015] NIQB 11
[240] Art 23 DPD
[241] *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB)
[242] Hurst, *supra nota 230,* at 191
[243] *L'Oreal v eBay*, para 144
[244] *Mosley v Google Inc* [2015] EWHC 59 (QB)

Hurst suggests that if the two directives can be read in harmony in interpreting the general monitoring obligation, courts will likely have to take into account Article 7 (the right to respect for private and family life), Article 8 (right to the protection of personal data) and Article 47 of the EUCFR (right to an effective remedy).[245] For example, the England and Wales Court of Appeal held in *Benkharbouche and Janah v Embassy of Sudan* that the right to an effective remedy for a breach of a right granted under EU law is a general principle of EU law.[246] This indicates that privacy rights under EU law are achieving a kind of an elevated status under EU law and EU citizens have a guaranteed right to an effective remedy to prevent privacy violations, even if that remedy is very much like a general monitoring obligation. This seems to be the case no matter whether the privacy right is framed in data protection or fundamental rights terms.[247]

[245] Hurst, *supra nota 230,* at 193
[246] *Benkharbouche v Embassy of Sudan* [2015] EWCA Civ 33, at [69]–[85]
[247] Hurst, supra nota 230, at 193

## 4. Freedom of Expression

Freedom of expression has been described as one of the obvious boundaries between relatively open and closed societies, between liberal democracies and different types of authoritarian regimes.[248] Already in 1516 Erasmus wrote that in "a free state, tongues should be free too". In 1770 Voltaire noted that "I detest what you write, but I would give my life to make it possible for you to continue to write" and in 1859 John Stuart Mill wrote in his essay On Liberty "if any opinion is compelled to silence, that opinion may, for aught we can certainly know, be true. To deny this is to assume our own infallibility".[249]

Nonetheless, it took until 1948 for the right to freedom of expression to be formally codified in the Universal Declaration of Human Rights (UDHR). According to its Article 19, everyone has the right to freedom of expression and opinion, which includes the freedom to hold opinions without interference and the right to seek, receive and impart information and ideas through any media regardless of frontiers. Today, the right is also guaranteed in several other international legal instruments, such as in Article 19 of the International Covenant on Civil and Political Rights (ICCPR), Article 10 of the ECHR and in Article 11 of the EU Charter.

### 4.1. Freedom of Expression in the European Legal Order

The European Court of Human Rights (ECtHR) has emphasised the essential role of freedom of expression in any democratic society since it is "one of the basic conditions for its progress and for the development of every man".[250] This points to the dual role that freedom of expression plays in the European legal system. On the one hand, it allows individuals to disclose, communicate and compare their thoughts, opinions and ideas and have access to information, and on the other hand, freedom of expression affects the democratic quality of the overall political, cultural or economic system.[251] Furthermore, the right to freedom of expression is one of the essential foundations of a

[248] Alston, P. & Goodman, R. International Human Rights – Text and Materials. 1st edn. Oxford: Oxford University Press 2013, p.651
[249] Smith, D. and Torres, L. Timeline: a history of free speech (The Guardian 5 Feb 2006) http://www.theguardian.com/media/2006/feb/05/religion.news (14.03.2016)
[250] ECtHR, *Handyside v the United Kingdom* (Application no. 5493/72, 1976), para 49
[251] Barata Mir, J. and Bassini, M. Freedom of Expression in the Internet – Main Trends of the Case Law of the ECtHR, p.78 in 'The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe, edited by Oreste Pollicino and Graziella Romeo (Routledge 2016 Oxford)

democratic society and it is not only applicable to information or ideas that are "favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb".[252] Although the freedom is subject to exceptions, these must be "construed strictly, and the need for any restrictions must be established convincingly".[253] Such a reasoning is directly connected to one of the limits that restrictions to freedom of expression must meet according to Article 10(2) ECHR, namely the existence of a compelling social need in a democratic society. Consequently, Article 10 of the ECHR will offer protection to any expression that contributes to the strengthening and development of the democratic system while putting aside the potential negative and disruptive effects.[254] Furthermore, the ECtHR has made clear that the provision protects speakers from state interference, but at the same time, also imposes certain positive obligations in order to ensure media freedom and provide the conditions for a real and effective exercise of such rights.[255]

It should also be noted that although Article 10 of the ECHR is considered to be the leading source for the protection of freedom of expression in Europe, the influence of two other factors should also be taken into account. Firstly, the incorporation of the EUCFR into EU primary law has resulted in ranking its Article 11 (freedom of expression and information) amongst the fundamental rights which are formally protected by the EU.[256] Also, according to Article 6(2) of the Treaty on European Union (TEU), the Union is required to accede to the ECHR even though all 28 EU Member States are already individually party to the Convention. Secondly, although the EU was originally intended to create an economic community only, in more recent times, it has acquired a new supranational dimension as a non-economic community. This has resulted in the CJEU delivering rather remarkable decisions that, despite their main focus of assessing the conformity with EU law, have brought with them substantial implications for the protection of freedom of expression. This development can especially be seen in cases involving internet and new technologies, such as the aforementioned *Google Spain* case, which offered crucial implications to the protection of freedom of expression in the online world.[257] However, regardless of the CJEU entering the arena of fundamental rights protection, it has constantly had regard to

[252] ECtHR, *Handyside v the United Kingdom* (Application no. 5493/72, 1976) para 49
[253] ECtHR, *Zana v Turkey* (Application no. 69/1996/688/880, 1997) para 51
[254] Barata Mir, J. and Bassini, M. *supra nota 251* p.79
[255] ECtHR, *Özgur Gündem v Turkey* (Application no. 23144/93, 2000) para 42
[256] Jääskinen, N. The Place of the EU Charter within the Tradition of Fundamental and Human Rights. In Fundamental Rights in the EU: A Matter for Two Courts / edited by Sonia Morano-Foadi and Lucy Vickers (Oxford: Hart Publishing 2015, pages 11-20)
[257] Barata Mir, *supra nota 230* p.77

the ECHR and has repeatedly held that the Convention holds special significance for EU law.[258] The EUCFR also contains a number of provisions that mirror the language of the ECHR and according to Article 52(3) of the Charter those provisions have an identical scope. Therefore, the ECHR and the extensive case law of the ECtHR provides the most comprehensive overview of the protection of freedom of expression in Europe.

### 4.2. Freedom of Expression on the Internet

Internet publications fall within the scope of Article 10 of the ECHR, but the particular nature of the medium has led the ECtHR to rule on certain restrictions that have been imposed on freedom of expression on the internet.[259] The Court stated in the case *Editorial Board of Pravoye Delo and Shtekel v Ukraine* that internet is an information and communication tool that is distinct from printed media, especially with regard to the capacity to store and transmit information. Thus, the risk of harm posed by content and communications on the internet to the exercise and enjoyment of human rights and freedoms, in particular the right to privacy, is without a doubt higher than posed by the traditional press.[260] Accordingly, internet is not, and potentially will never be, subject to the same regulations and control than printed media.[261] In cases concerning online publications the Court has stressed internet's vital role in facilitating access to information. Due to the accessibility and capacity to store and communicate extensive amounts of information, internet plays a significant role in enhancing the public's access to news and simplifying the dissemination of information.[262] However, the right to freedom of expression is not absolute. In *K.U. v Finland*, the ECtHR held that although freedom of expression and confidentiality of communications are the main considerations and users of communications services must have guarantees that their own privacy and freedom of expression online will be respected, the guarantee cannot be without limits and must, under certain circumstances, give away to other legitimate concerns such as the prevention of crime and disorder or the protection of the rights and freedoms of other.[263]

[258] Oliver, P. Companies and their fundamental rights: a comparative perspective I.C.L.Q. 2015, 64(3), 661-696, at 676
[259] Research Division of the European Court of Human Rights. Internet: case-law of the European Court of Human Rights. www.echr.coe.int/Documents/Research_report_internet_ENG.pdf (14.03.2016)
[260] ECtHR, *Editorial Board of Pravoye Delo and Shtekel v Ukraine* (Application no. 33014/05, 2011) para 63
[261] ECtHR, *Wegrzynowski v Poland* (Application no. 33846/07, 2013) para 58
[262] ECtHR, *Times Newspapers Ltd. (nos. 1 and 2) v United Kingdom* (Application no. 3002/03 and 23676/03, 2009)
[263] ECtHR, *K.U. v Finland* (Application no. 2872/02, 2008) para 49

One of the elements that the ECtHR examines in assessing the legality of limitations to freedom of expression is the necessity of such a measure in a democratic society. Such an assessment implies the application of a proportionality test with the aim of avoiding restrictions whose aims are legitimate but which nevertheless constitute an excessive and unnecessary restriction on protected expression.[264] The *Yildirim v Turkey* case concerned an order by a Turkish criminal court to block a website hosted by Google Sites accused of insulting the memory of Ataturk. The order, however, was extended, for the apparent reason that it was the only means of blocking the offending website, to all Google sites from Turkey. The Court found a violation of Article 10 and held that Turkish law should lay down obligations for the domestic courts to examine whether the wholesale blocking of Google sites was necessary and that the law should ensure tight control over the scope of any such bans to ensure that the least restrictive measure is applied.[265]

The ECtHR has also held, in a case involving the freedom of expression of journalists on the internet, that a State has a positive obligation towards guaranteeing the right. The judgment in the case *Editorial Board of Pravoye Delo and Shtekel v Ukraine* was the first time that the Court acknowledged that Article 10 had to be interpreted as imposing on States a positive obligation to create an appropriate regulatory framework for ensuring effective protection of the freedom of expression of journalists on the internet.[266] The case concerned a defamation suit against a newspaper and its editor-in-chief for publishing a report on political corruption based on a source downloaded from the internet. The ECtHR, in finding a violation of Article 10, held that the absence of specific national provisions, which allow journalists to use information obtained from the internet without fear of incurring serious sanctions, severely hinders the exercise of the crucial role of the press as a public watchdog.[267]

Moreover, the Court has also been required to assess cases concerning internet archives and the removal of information from the public domain, facts which are somewhat similar to the circumstances in the CJEU's *Google Spain* judgment. In *Times Newspapers Ltd. (nos. 1 and 2) v United Kingdom* the ECtHR stressed that the maintenance of internet archives is a crucial aspect of internet's vital role in facilitating access to information and such archives fall within the ambit of protected expression guaranteed by Article 10 of the ECHR.[268] Furthermore, in *Wegrzynowski*

[264] Barata Mir, *supra nota 230,* p.83
[265] ECtHR, *Yildirim v Turkey* (Application no. 3111/10, 2012)
[266] ECtHR, *Editorial Board of Pravoye Delo and Shtekel v Ukraine* (Application no. 33014/05, 2011) para 64
[267] Ibid, para 46
[268] *Times Newspapers Ltd. (nos. 1 and 2) v United Kingdom*, para 27

*v Poland* the Court noted that it is not the role of judicial authorities to participate in rewriting history by ordering the removal from the public domain of all traces of publications which have sometimes in the past been found to constitute unjustified attacks on an individual's reputation.[269] The decision, which has been called the ECtHR's own 'right to be forgotten' ruling,[270] concerned a complaint about a newspaper article that was still accessible on the newspaper's website although the Polish courts had previously found the paper version to constitute libel. The ECtHR held that the Polish courts had struck a fair balance between the general public's right to access to information in comparison to the applicant's right to have his reputation protected by not requiring the newspaper to remove the article from their archives.[271]

Likewise, in the *Max Mosley v the United Kingdom* case, the ECtHR rejected the argument that the Article 8 right to private life includes a requirement for pre-notification of intended publication referring to an individual's private life. Although the judges acknowledged the potential impact of such information and the difficulty of removing it from the internet even if required by a court order, Article 10 sets out a limited scope for restrictions on the freedom of the press to publish material which contributes to public debate on matters of general public interest.[272] This coupled with the chilling effect that a pre-notification requirement risks giving rise to as well as the substantial doubts regarding the effectiveness of such requirements led the Court to dismiss the application.[273] As a whole, the above case law demonstrates the broad interpretation that the ECtHR has given to the right to freedom of expression on the internet, especially in cases involving journalistic activities.

### 4.3. Companies and Their Fundamental Rights

In addition to a wide interpretation of the scope of the right to freedom of expression, the ECtHR has also adopted a broad meaning of those who may rely on it. Unlike with data protection, legal persons, such as companies and associations, can also claim violations of their human rights under the ECHR system. According to Article 34, corporations and other private legal persons may

[269] ECtHR, *Wegrzynowski and Smolczewski v Poland* (Application no. 33846/07, 2013) para 65
[270] Frantziou, E. Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*. Human Rights Law Review, 2014, 14, 761–777, at 772
[271] *Wegrzynowski v Poland (supra nota 269)* para 68
[272] ECtHR, *Max Mosley v United Kingdom* (Application no. 48009/08, 2011) para 130
[273] *Max Mosley v United Kingdom*, paras. 131-132

submit cases on their own behalf to the ECtHR, although only in cases where the claimant can qualify as a victim, meaning that the legal person must be directly affected by the act or omission in the particular case.[274] Therefore, at least under the ECHR system, internet intermediaries can rely on the right to freedom of expression. This was recently confirmed by the ECtHR in the *Delfi* case.[275]

The case involved an article about the actions of a local ferry company posted on Delfi, one of the largest internet news portals in Estonia, and user comments posted under that article. Six weeks after the publication of the article, the company's majority shareholder requested the removal of 20 comments since they were allegedly defamatory and Delfi complied with the request on the same day.[276] Despite the removal of the comments, Estonian courts, including the Supreme Court, held Delfi liable for a 320 euro fine since the portal did not qualify as an intermediary under the Estonian Information Society Services Act (ISSA), which transposed the e-Commerce Directive into national law since it is a content provider that actively invites users to comment on its platform with the aim of obtaining financial gain.[277] Delfi claimed before the ECtHR that imposing civil liability on them for comments posted by third parties constituted a violation of their freedom of expression and freedom to impart information. However, both the First Section and the Grand Chamber of the ECtHR held that there had been no disproportionate restriction on Delfi's Article 10 rights.

The Grand Chamber based its decision on attempting to strike a balance between Article 8 and Article 10 of the ECHR that would retain the essence of both rights.[278] The Court recognised that the duties of internet news portals with regard to third party content may differ to a certain degree from those of a traditional publisher, who acts as an editor to all the content that appears in its publication.[279] Further, the Court took care to strictly limit its holding to a large professionally managed internet news portal which runs on a commercial basis, publishes articles on its own and invites readers to submit comments on them.[280] Thus, the principles laid out in the decision do not apply to other fora such as social media platforms or internet discussion forums and bulletin

[274] Van Kempen, P. Human Rights and Criminal Justice Applied to Legal Persons. Protection and Liability of Private and Public Juristic Entities under the ICCPR, ECHR, ACHR and AfChHPR. Electronic Journal of Comparative Law, vol. 14.3 (December 2010), http://www.ejcl.org/143/art143-20.pdf (12.03.2016)
[275] ECtHR, *Delfi AS v Estonia* (Application no. 64569/09, 2015)
[276] *Delfi AS v Estonia* paras 16-20
[277] Estonian Supreme Court. *Vjatšeslav Leedo v AS* Delfi (Case no. 3-2-1-43-09, 2009), para 13
[278] *Delfi AS v Estonia*, para 110
[279] Ibid, para 113
[280] Ibid, para 115

boards.[281] Finally, although the Estonian courts had classified the user comments as defamatory, the Grand Chamber found them to constitute hate speech or incitement to violence against the company's majority shareholder, categories of speech which are not protected under the Convention.[282]

Less than a year after the *Delfi* judgment, the Fourth Section of the ECtHR delivered a ruling on nearly identical facts in *MTE and Index v Hungary* case.[283] This time, however, they decided the other way, namely that Hungarian courts had violated Article 10 ECHR by placing strict liability on a news portal for reputational harm caused by user comments. The judgment involved MTE, the self-regulatory body of Hungarian internet content providers and Index, the owner of one of the largest internet news portals in Hungary, both of whom allowed user comments on the publications appearing on their portals.[284] MTE published an article criticising the business practices of two real estate websites and Index in turn wrote about that article and copied its full text, with both articles attracting comments from users attacking the real estate websites.[285] Consequently, the two real estate websites brought a civil claim against MTE and Index arguing that the article and subsequent comments have infringed their good reputation.[286] The Hungarian courts found MTE and Index liable for, what in their opinion were injurious, offensive and unlawful user comments.[287] Similarly as in the Delfi case, the domestic courts excluded the application of Act no. CVIII of 2001, which transposed the ECD into Hungarian law, but on the grounds that the Act only related to electronic services of a commercial nature, particularly to purchases through the Internet, while the comments in question were private assertions.[288]

Unlike in the *Delfi* case, however, the ECtHR found that the Hungarian courts had violated the applicants' right to freedom of expression enshrined in Article 10 of the ECHR. The Fourth Section's ruling was based on the opinion that the Hungarian courts had not carried out a proper balancing exercise between the competing rights involved, namely the applicants' right to freedom of expression and the real estate websites' right to respect for their commercial reputation.[289] The

[281] Ibid, para 116
[282] Ibid, para 117
[283] ECtHR. *Magyar Tartalomszolgáltatók Egyesülete & Index.hu ZRT v Hungary* (Application no. 22947/13, 2016)
[284] Ibid, paras 5-6
[285] Ibid, paras 12-14
[286] Ibid, para 15
[287] Ibid, para 22
[288] Ibid, para 20
[289] Ibid, para 88

Court also made a point of differentiating the case from *Delfi* on the account of the comments in *MTE and Index* not amounting to hate speech and direct threats to individuals.[290]

Due to the similarities between the factual situations and the different outcomes of the two cases, a closer examination of the ECtHR's reasoning is warranted. In both cases it was uncontested that the applicants' rights under Article 10 ECHR had been interfered with by the domestic courts' decisions. In considering whether such interferences with the right to freedom of expression were justified, the ECtHR analysed whether three cumulative conditions had been satisfied. First of all, whether the restriction was prescribed by law; secondly, whether the interference had one or more legitimate aims; and thirdly, whether the restriction was necessary in a democratic society.[291]

### 4.3.1. Prescribed by Law

According to the case of law of the ECtHR, the expression "prescribed by law" in Article 10(2) requires, in addition to the challenged measure having a legal basis in domestic law, also that the law be accessible to the person concerned and foreseeable as to its effects. Nonetheless, according to the ECtHR, it is principally up to the national authorities, especially the courts, to interpret and apply domestic law.[292] The condition of foreseeability entails that the law in question is sufficiently precise in order to enable the citizen to regulate his conduct and be able to foresee, to a reasonable degree, the consequences that a given action may lead to. Notably, the consequences do not have to be foreseeable with absolute certainty, since the law must also be able to keep up with changing circumstances.[293]

In *Delfi*, the applicant argued that the interference with its rights under Article 10 was not prescribed by law because there was no legislation or case law declaring that an intermediary was to be considered as the publisher of content which it was not aware of. They relied on the ECD and ISSA stating that the applicable law specifically prohibited the imposition of liability on service providers for third party content where, upon obtaining actual knowledge of illegal activities, they expeditiously removed or disabled access to the infringing content.[294] The

[290] Ibid, para 91
[291] Article 10(2) ECHR. See also MTE para 46 and Delfi para 119
[292] Delfi, para 120.
[293] Delfi, para 121
[294] Delfi, para 69

Government, on the other hand, referred to the relevant provisions of the civil law to the effect that media publishers were liable for their publications together with the authors and asserted that there was no Estonian case law on the basis of which Delfi could have assumed that the owner of an internet news portal was not liable for the damage caused by comments posted on its articles, especially since the comments formed an integral part of the news which only Delfi could administer.[295] The Grand Chamber stated that they could only assess whether the interpretations by the Estonian courts were compatible with Article 10(2) and not whether the legislation that the domestic courts had found to be applicable was correct.[296] The Court observed that the differences in the parties' arguments were based on their diverging views on the classification of Delfi as either a media publisher or an intermediary with respect to the user comments.[297] The Grand Chamber, however, did not clarify which category Delfi belongs to and concluded that the interference in question was prescribed by law within the meaning of Article 10(2) as Delfi, as a professional publisher, should have been familiar with the domestic legislation and case law and could have also sought legal advice.[298]

In *MTE and Index*, the parties' opinions also differed as to whether the interference was prescribed by law. The applicants based their arguments on the e-Commerce Directive's liability exemptions for hosting providers while the Hungarian Government contended that private expressions, such as the impugned comments fell outside the scope of the liability exemption and relied on the Civil Code stating that the applicants were liable for disseminating private third-party opinions.[299] Like in Delfi, the ECtHR reiterated that its task was not to take the place of domestic courts and it was confined to examining whether the domestic courts' application of national law was foreseeable for the purposes of Article 10(2).[300] They concluded that the applicants were in a position to have been able to foresee, to a reasonable degree, the consequences which their activities could entail and therefore the interference in issue was prescribed by law.[301]

[295] Delfi, para 84
[296] Delfi, para 85
[297] Delfi, para 123
[298] Delfi, para 129
[299] MTE and Index, para 47
[300] MTE, para 49
[301] MTE, para 51

### 4.3.2. Legitimate Aim

The different legitimate aims for interference with the right are outlined in Article 10(2) ECHR and include "the interests of national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary". In *Delfi* there was no dispute between the parties that the restriction to the company's freedom of expression had pursued the legitimate aim of protecting the reputation and rights of others.[302] Likewise, in *MTE and Index*, the Hungarian Government submitted that the interference had as its aim the protection of the rights of others and the ECtHR saw no reason not to accept this.[303]

### 4.3.3. Necessary in a Democratic Society

When assessing whether an interference is necessary in a democratic society, the ECtHR began the analysis with a consideration of the fundamental principles. Freedom of expression is one of the essential foundations of a democratic society and restrictions to it must be narrowly construed. The term "necessary" implies the existence of a pressing social need and although Member States have a certain margin of appreciation in determining whether such a need exists, this goes hand in hand with European supervision. Thus, the ECtHR is empowered to give the final ruling on whether a restriction can be reconciled with freedom of expression. Moreover, the Court has to look at the specific restriction complained of in the light of the case as a whole and assess whether it is proportionate to the legitimate aim pursued and whether the reasons shown by the national authorities to justify it are relevant and sufficient.[304] In addition, according to the case law of the Court, the right to protection of reputation is covered by Article 8 of the ECHR, although in order for it to come into play, the attack on a person's reputation must attain a certain level of seriousness.[305] In examining whether there is a need for an interference with freedom of expression in a democratic society with the aim of protecting the reputation or rights of others, the ECtHR

[302] Delfi, para 130
[303] MTE, para 52
[304] Delfi, para 131 and MTE, para 54
[305] Delfi, para 137 and MTE, para 57

may be required to evaluate whether the domestic authorities have struck a fair balance between the right to freedom of expression and the right to respect for private life.[306]

In *Delfi*, the Court held that the majority of the impugned comments amount to hate speech or incitements to violence, and as a result, they did not enjoy the protection of Article 10.[307] In order to decide whether the domestic courts' decisions of holding Delfi liable for comments authored by third parties violated its freedom of expression, the Grand Chamber adopted the factors considered by the First Section, namely the context of the comments, the measures applied by Delfi in order to prevent or remove the defamatory comments, the liability of the actual authors as an alternative, and the consequences of the domestic proceedings for Delfi.[308] With regard to context, Delfi had exercised a substantial degree of control over the comments published, thus its involvement went beyond that of a passive and purely technical service provider.[309] Delfi had rules in place for the comment section and deleted comments if these rules were breached. Also, the authors of the comments could not modify or delete their comments after posting.[310]

As for the liability of the actual authors, the ECtHR accepted that it was extremely difficult to identify the authors, but Delfi had not done anything to make it possible for a victim of hate speech to effectively bring a claim against the actual authors of the comments since it allowed anonymous posting.[311] Furthermore, the comments were clearly unlawful and since Delfi highlighted the most commented thread, it should have been aware of the places on its website with the liveliest exchange and had an obligation to take measures to limit the dissemination of hate speech and speech inciting to violence.[312] Even though Delfi had in place an automatic word-based filtering system and a notice and take-down procedure, these had failed to filter out the unlawful comments.[313] As to the consequences for Delfi, the ECtHR held that an award of €320 was not disproportionate to the breach and they had not had to change their business model as a result.[314] Based on the above assessment, the Grand Chamber concluded that the imposition of liability did

[306] Delfi, para 138 and MTE, para 58
[307] Delfi, para 140
[308] Delfi, para 142
[309] Delfi, para 146
[310] Delfi, 155
[311] Delfi, 150-151
[312] Delfi, 152-155
[313] Delfi, 156 and 159
[314] Delfi, 160-161

not constitute a disproportionate restriction on Delfi's right to freedom of expression and there had been no violation of Article 10 of the ECHR.[315]

In *MTE and Index*, the ECtHR also had to examine whether the domestic courts' decision to impose liability on the applicants for third-party comments was based on relevant and sufficient reasons in the given circumstances of the case. They based their assessment on similar factors as in *Delfi* though adding the criterion of the consequences of the comments for the injured party as well as also considering the content of the comments. First of all, the Court differentiated the two cases on the basis that the comments in *MTE and Index*, although offensive and vulgar, did not amount to hate speech or incitement to violence, that MTE, as a non-profit self-regulatory body, had no economic interests, and that the plaintiffs were legal persons.[316] With regard to the context of the comments, the Court noted that the underlying article, which featured the unethical practices of the real estate websites was in the public interest and the user comments could be considered as going to a matter of public interest.[317] The ECtHR acknowledged that although the expressions used in the comments were offensive, they belonged to a low register of style, which is common in communication on internet portals, which in turn reduced the impact that could be attributed to them.[318]

As to the liability of the authors of the comments, the domestic courts had not given any consideration as to whether they could be identified and held liable, and liability was imposed on the applicants because they had disseminated defamatory statements. The ECtHR considered the applicants' activities to be journalistic and thus their liability did not fit with the existing case law according to which punishing a journalist for the dissemination of statements made by others in an interview would significantly hamper the contribution of the press to matters of public interest.[319] With regard to measures taken by the applicants, the Court remarked that the applicants had immediately removed the comments from their websites upon notification of the civil proceedings. Also, the Court observed that the applicants took certain measures to prevent defamatory comments, which included a disclaimer stipulating that the authors were accountable for the comments and posting comments injurious to the rights of third parties was prohibited, a notice and take-down system, which the real estate websites had failed to use and, in the case of

[315] Delfi, para 162
[316] MTE, paras 69-70
[317] MTE para 72
[318] MTE, paras 76-77
[319] MTE, para 79

Index, also a team of moderators who performed partial follow-up moderation of user comments.[320] As to the consequences, the ECtHR observed that at the time of publication of the article and the impugned comments, there were ongoing complaints about the real estate websites' business conduct and therefore, the Court was not convinced whether the comments in question were capable of having any additional or significant impact. Besides, the Hungarian courts had not evaluated whether the comments reached the requisite level of seriousness and whether they had actually caused prejudice to a legal person's right to professional reputation.[321] With regard to the consequences for the applicants, although the domestic courts had not made an award for damages and only obliged the applicants to pay the websites' court fees and legal costs, the mere fact of finding website operators liable for user comments was likely to have a chilling effect on freedom of expression.[322]

The fact that the Hungarian courts had not paid any attention to how the application of civil liability to a news portal operator will affect freedom of expression on the internet called into question the adequacy of the protection of the applicants' freedom of expression rights at the domestic level.[323] On account of the above analysis, the ECtHR concluded that the rigid stance of the domestic courts effectively precluded the carrying out of a balancing exercise between the two competing rights in accordance with the Court's case law, which constituted a sufficient justification for concluding that there had been a violation of Article 10.[324]

### 4.4. Current State of Intermediary Liability for User-Generated Content under the ECHR

In the concurring opinion in *MTE and Index*, Judge Kūris explained that despite the different outcomes, the *MTE and Index* judgment does not depart from the principles established in the *Delfi* ruling. The comments in *MTE and Index* were merely vulgar and offensive and did not amount to hate speech and incitement to violence and therefore could not *a priori* be viewed by the applicants as clearly unlawful.[325] However, differentiating between comments that are clearly unlawful and ones which merely belong to a low register of style and are common in communication on many

[320] MTE, para 81
[321] MTE, para 85
[322] Delfi, para 86
[323] MTE, para 88
[324] MTE, paras 89-91
[325] MTE and Index, Concurring Opinion of Judge Kūris, para 2

internet portals is not very straightforward. It is not clear to the author why comments such as "rascal" and "a good man lives a long time, a shitty man a day or two"[326] are clearly unlawful while a comment like "people like this should go and shit a hedgehog and spend all their money on their mothers' tombs until they drop dead"[327] is merely offensive and defamatory. The author acknowledges that in *Delfi* there was one comment that was plainly racist and anti-Semitic and thus could be classified easily as clearly unlawful. However, the rest of the 20 comments in question are essentially undistinguishable from the type of comments in *MTE and Index*. It is undisputable that defining the exact limits of hate speech and incitement to violence is extremely difficult, especially in the context of the internet. Nevertheless, as also pointed out by Judges Sajó and Tsotsoria in their dissent, the Court in *Delfi* blatantly ignored the question on what grounds and to what extent do the comments amount to hate speech and constitute a real threat to a persons' life. They simply accepted the Estonian Supreme Court's finding that the illegality of the comments is manifest.[328] If the Grand Chamber of the ECtHR cannot or will not give any guidance on separating clearly unlawful comments from merely offending and vulgar ones, how is the operator of a website supposed to be able to do it? This is especially confusing since a statement may be defamatory without being unlawful because a comment which destroys a man's reputation is only unlawful if it is not true.[329]

In addition, in the *MTE and Index* case, the Court crucially held that implementing a NTD system accompanied by effective procedures allowing for rapid response is sufficient to balance the rights and interests of the parties involved. Thus, such a system would have been sufficient for protecting the commercial reputation of the plaintiff.[330] This interpreted in combination with the *Delfi* ruling, means that it is acceptable if offensive comments are deleted upon notification, while higher standards of care need to be applied to hate speech and incitement to violence, which requires portals to remove material on their own initiative. The Court, however, did not address the issue that in order to detect hate speech, monitoring of all comments will most likely need to be done. This, in turn, runs the risk of leading into general monitoring, which is explicitly prohibited under Article 15 of the ECD, except in specific cases and with an order by a national court or

[326] Delfi, para 18
[327] MTE, para 14
[328] Joint Dissenting Opinion of Judges Sajó and Tsotsoria in *Delfi AS v Estonia* (supra nota ), para 14
[329] Weinert, E. MTE v Hungary: the first European Court of Human Rights ruling on liability for user comments after Delfi AS v Estonia. Ent. L.R. 2016, 27(4), 135-139, at 138
[330] MTE, para 91.

administrative authority.[331] Consequently, employees looking for *Delfi*-level comments that are clearly unlawful will inevitably come across other user-generated content that might reach *MTE*-level defamation. Despite the fact that according to the ECtHR intermediaries cannot be required to look for the latter, once employees see them, they will presumably be removed as well.[332] This results from the requirement set out in Article 14 of the e-Commerce Directive that once an intermediary gains knowledge of unlawful content, whether via notice or other means, it must expeditiously remove it. By virtue of not being able to assess the truth of the disputed facts, employees of internet intermediaries are put into an impossibly difficult position to make legal judgments that even courts find complicated. This will most likely lead to over removal of content just to be safe and avoid liability.[333] The conclusion then seems to be that Articles 14 and 15 of the ECD offer online intermediaries more protection than Article 10 of the ECHR.

[331] Ombelet, P.J. and Kuczerawy, A. Delfi revisited: the MTE-Index.hu v. Hungary case http://blogs.lse.ac.uk/mediapolicyproject/2016/02/19/delfi-revisited-the-mte-index-hu-v-hungary-case/ (07.04.2016)
[332] Keller, D. Policing Online Comments in Europe: New Human Rights Case Law in the Real World (12 April 2016) https://cyberlaw.stanford.edu/blog/2016/04/policing-online-comments-europe-new-human-rights-case-law-real-world (21.04.2016)
[333] Ibid

# 5. Future of Intermediary Liability

## 5.1. Reconciling the Three Separate Intermediary Liability Regimes

The present thesis is founded upon the premise that currently in Europe there are three separate regimes that govern the liability of internet intermediaries for content created by their users. These are the e-Commerce Directive, the Data Protection Directive and the right to freedom of expression. Although each regime seemingly has their own specific field of application, they also tend to overlap, which has resulted in legal uncertainty, inequality and confusion, since each system creates specific obligations for internet intermediaries. The question thus arises whether the future of intermediary liability lies in reconciling the application of the current three regimes with each other.

The common thread running through the case law of all the three regimes is that they shift the responsibility for deciding whether certain content is unlawful from state authorities to private entities. In order to benefit from the liability exemption in Article 14 of the ECD, a hosting provider is required to take down illegal information upon obtaining actual knowledge or awareness of it. Accordingly, an intermediary will have to make the assessment over whether particular content is in fact illegal. Likewise, under the Data Protection Directive, if an intermediary is considered to be a data controller, it then has the obligation to consider whether particular content is unlawful and should be removed, or more precisely, forgotten. Finally, also under the right to freedom of expression the assessment of whether particular user content is unlawful and should thus be removed is left to the intermediaries that allow the posting of UGC.

Such removal of content is achieved through variations of a notice and take-down system. This derives from the knowledge based liability regime whereby intermediaries are only bound to react to complaints after receiving notification of illegal content as set out in Article 14 of the ECD. A similar mechanism is also endorsed by the ECtHR's decision in *MTE and Index,* where the Court held that implementing a NTD system which is accompanied by a rapid response is sufficient to balance the rights and interests of the parties involved. The problem with the NTD system is that neither the e-Commerce Directive, nor the CJEU or ECtHR in their case law have set out any detailed rules for the procedure, which has resulted in widely differing interpretations in the EU Member States. This issue could be addressed by setting out detailed rules for the system on a

European wide level. The US DMCA offers some examples of what these rules could entail. For example they should set out the elements that an adequate notification should include, such as information identifying the author of the complaint, the exact location and content of the infringing post, contact information of the author of the complaint and a statement that the information in the notification is correct. Also, the rules should outline that an intermediary service provider should have a designated agent to receive notifications of claimed violations, whose contact details should be easily identifiable on the platform.[334] Such rules could make the NTD process more clear for both the intermediaries as well as the victims of unlawful content.

However, the overall concern still remains as making internet intermediaries responsible for the unlawful content hosted on their platforms effectively places the burden of establishing whether that content really is illegal also on the intermediaries, which in turn runs the risk of favouring an excessively cautious attitude by the intermediary, who would be forced into censorship measures whenever there is the smallest risk of a judicial decision in favour of a take-down, thus unduly restricting freedom of expression and threatening innovation. Moreover, there is also the danger that those who want to prevent the distribution of information about themselves will threaten to sue intermediaries for privacy violations with the aim of inducing the intermediaries to censor the content in question, even in situations when it expresses legitimate criticism.[335] Such a situation has been called for example private censorship,[336] censorship-by-proxy,[337] collateral censorship,[338] and privatised censorship[339].

This development has also been noted by the UN Special Rapporteur Frank La Rue, who stated that since intermediaries may still be held financially, or in some cases even criminally, liable if they do not remove content upon receipt of notification regarding unlawful content, they are prone to err on the side of safety by over-censoring potentially infringing content.[340] This coupled with the lack of transparency in the intermediaries' decision-making process poses a risk to freedom of expression online. Intermediaries, as private entities, are not best placed determine whether

[334] Van Der Sloot (2015), supra nota , paras 52-53
[335] Azevedo Cunha, Marin & Sartor, (supra nota 2) at 66
[336] Ibid
[337] Keller. Intermediary Liability (supra nota 5)
[338] Joint Dissenting Opinion of Judges Sajó and Tsotsoria in *Delfi AS v Estonia*, para 1
[339] Edwards. Fall and Rise, (supra nota 6) p.74
[340] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue on the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet (A/HRC/17/27, 16 May 2011), para 42
http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (19.01.2016)

particular content is illegal, which requires a careful consideration and balancing of competing interests and application of defences. Therefore, the Special Rapporteur concludes that censorship measures should never be delegated to a private entity, and further, no one should be held liable for content of which they are not the author.[341]

In this regard it is also worth noting the immense power that technology giants, such as Google and Facebook have. Just five companies account for nearly two-thirds of revenue from advertising on the web while "the open internet accounts for barely 20% of the entire web with the rest of it hidden away in unsearchable 'walled gardens' such as Facebook, whose algorithms are opaque, or on the 'dark web', a shady parallel world wide web".[342] It has even been suggested that technology giants have taken on certain state-like characteristics. For example, while governments issue their citizens with passports, identity cards and driver's licences to verify identity, our online IDs are provided by Google, Facebook and Apple. Moreover, Microsoft has a foreign service that negotiates with foreign governments and Facebook has its own internal counter-terrorism unit. Bernal goes as far as saying that these technology companies are the new wave of colonisation as they are creating their own empires.[343] This has resulted in the private sector gaining exceptional influence over the freedom of expression and information of individuals. Therefore, the collection and storage of information by entities with such dominant and important internet presences especially gives rise to concerns of accountability and transparency in their decision-making over what content to remove.[344]

The issue of private censorship and the debate over how these powerful private companies control free expression online is interesting in the light of another fundamental right, namely the freedom to conduct a business in accordance with EU law and national laws and practices, enshrined in Article 16 EUCFR. For example, the *Delfi* judgment put a lot of emphasis on the economic nature of the portal's activity in justifying the imposition of liability for the user-generated comments. This is in direct contrast with Recital 18 of the ECD, which states that a hosting service provider is not automatically excluded from the scope of the ECD if the service forms part of an economic

[341] Ibid, para 43
[342] Malcomson, S. Growing up: How the internet lost its free spirit (The Economist, 26 March 2016) http://www.economist.com/news/books-and-arts/21695370-how-internet-lost-its-free-spirit-growing-up (31.03.2016)
[343] Hodson, H. Apple vs FBI: Who will win this struggle for power? (New Scientist, 22 February 2016) https://www.newscientist.com/article/2078419-apple-vs-fbi-who-will-win-this-struggle-for-power/ (31.03.2016)
[344] McGoldrick, D. Developments in the Right to be Forgotten (2013) 13 Human Rights Law Review 761-766, p.762

activity. Consequently, it seems that while making a profit does not disqualify an intermediary from the liability exemptions in the ECD, it will make it more difficult for intermediaries to rely on their freedom of expression. How this relates to the fundamental right to conduct a business is currently unclear since there have been no judgments considering the interaction of these two rights.[345]

Another negative consequence of imposing liability on intermediaries for UGC that the *Delfi* decision has demonstrated is the adverse influence on the right to anonymity online. By holding the portal liable on the grounds that it was impossible to ascertain the identities of the authors of the unlawful comments, the ECtHR effectively penalised Delfi for allowing anonymous user comments.[346] Thus, the ruling has the effect of curtailing anonymous internet speech since intermediary service providers will presumably be more reluctant to permit anonymous UGC on their platforms. This, in turn, is likely to result in either real-name registration policies, thereby undermining anonymity, or the elimination of posting UGC altogether on platforms that cannot afford to implement screening and moderating procedures, thus hurting smaller independent media.[347] The former has been the case in Estonia, where two major online news portals recently removed the possibility of anonymous commenting and now only allow comments by registered users.[348] This development is worrisome because anonymity plays an important role in safeguarding and advancing privacy, free expression, political accountability, public participation and debate.[349] On a positive note though the Delfi news portal still does allow anonymous user comments.

[345] Oliver, P. (2015) supra nota 258, p. 683
[346] McCarthy, H.J. supra nota 113, at 45
[347] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye on encryption, anonymity, and the human rights framework (A/HRC/29/32, 22 May 2015), para 54 http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
[348] These two news portals are ERR and Postimees. See: Isikutuvastamine ERR.ee kommentaariumis on nüüd ühekordne, end tuvastada saab ka mobiil-ID-ga (29 January 2016) http://uudised.err.ee/v/eesti/d631cdc9-8393-4fc1-8fd7-96f5260c7d41/isikutuvastamine-erree-kommentaariumis-on-nuud-uhekordne-end-tuvastada-saab-ka-mobiil-id-ga and Kangro, K. Postimees sulgeb veebruarist anonüümse kommentaariumi (30 December 2015) http://www.postimees.ee/3451469/postimees-sulgeb-veebruarist-anonuumse-kommentaariumi
[349] Report on encryption, anonymity, and the human rights framework, supra nota 347, para 47

## 5.2. EU Reform Plans and Proposals

### 5.2.1. The General Data Protection Regulation

After more than four years of negotiations, the final text of the General Data Protection Regulation[350] (GDPR) was finally adopted by the European Parliament on 14 April 2016. The GDPR will replace the Data Protection Directive and aims to make a uniform level of data protection throughout the EU a reality.[351] According to its Article 99, the GDPR will become applicable two years from the date of its entry into force, thus presumably in 2018.

Probably the most prominent provision of the GDPR is the Article 17 right to erasure ('right to be forgotten'), which requires data controllers to erase personal data without excessive delay if the personal data is no longer needed for its original purpose, if the data subject withdraws consent and where there is no other legal ground for processing, if the data subject objects to the processing and there are no overriding legitimate grounds for the processing, if the personal data has been unlawfully processed, if the personal data has to be erased in order to comply with EU or national legal obligations, and if the personal data has been collected in relation to offering information society services to children. Therefore, under Article 17 of the GDPR, intermediaries that are also considered to be data controllers are required to erase content based on the right to be forgotten (RTBF) requests.

The definition of a controller remains unchanged from the DPD, thus Article 4(7) of the GDPR defines a controller as „the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data“. However, the question that is left unanswered by the GDPR is whether intermediaries will count as data controllers with regard to RTBF removal obligations for content authored by their users.[352] Before the *Google Spain* decision the likely answer would have been that an intermediary is the processor while the user who uploaded the content is the controller. After the ruling, we now

[350] Regulation (EU) 2016/… of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf (29.04.2016)
[351] European Parliament Press Release: Data protection reform - Parliament approves new rules fit for the digital era (14 April 2016) http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era (17.04.2016)
[352] Keller, D. The Final Draft of Europe's "Right to Be Forgotten" Law (17 December 2015) http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law (17.04.2016)

know, that search engines are controllers for the purposes of data protection law. However, the question still remains with respect to other types of internet intermediaries. For example, Keller argues that it is highly unlikely that data protection authorities (DPA) will excuse major social networks from erasure obligations, at least in the long run.[353]

The most common argument against RTBF obligations for intermediaries is that they cannot be controllers because they only process content according to the wishes of the users, who are the actual controllers. In such a case if a data subject wishes to have personal data erased according to Article 17, the data subject should request the user to take it down, which would leave it up to the user to decide whether to remove the data or leave it on the platform and face the risk of a lawsuit. The data subject could also request the intermediary to take down the data, but since the intermediary is only a processor, the data subject could not rely on Article 17.[354]

If, however, both the intermediary and the user would be considered controllers with regard to UGC concerning third parties, the intermediary would be obliged to remove from its platform content uploaded by its users if the RTBF request complies with the conditions outlined in Article 17. This would result in intermediaries effectively becoming law enforcers for data protection, exercising this power-duty against their users, who would not be able to object and resist.[355] Moreover, it would mean that intermediaries that do not comply with the RTBF requests would be subject to crippling fines while there are no legal consequences for over-removal of content resulting from invalid RTBF requests.[356] The fines for RTBF violations, set out in Article 83(5) of the GDPR, amount "up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher". To put this into perspective, in 2015 Google's annual turnover was 74.54 billion USD[357] or around 65 billion EUR, thus making a 4% fine equal to about 2.6 billion EUR. It is an understatement to say that this creates a major incentive for intermediaries to comply with all removal requests that they receive. This would be extremely unfortunate given that both Bing and Google have reported that at least 50% of all RTBF requests that they receive are unfounded under EU law.[358]

---

[353] Ibid
[354] Sartor, G. Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? International Data Privacy Law, 2013, Vol. 3, No. 1, pp. 3-12, at 9
[355] Ibid, at 10
[356] Keller, D. The Final Draft of Europe's "Right to Be Forgotten" Law
[357] Annual revenue of Google from 2002 to 2015 http://www.statista.com/statistics/266206/googles-annual-global-revenue/ (21.04.2016)
[358] Keller, D. The Final Draft of Europe's "Right to Be Forgotten" Law

With regard to freedom of expression, the GDPR does state that it must be balanced with data protection and that RTBF requests can be denied on freedom of expression and information grounds.[359] Nevertheless, it does not provide any guidance on what exactly these grounds are. Rather, it leaves it to the EU Member States to reconcile, by law, the right to the protection of personal data with the right to freedom of expression and information.[360] This is problematic since it is the same allocation of responsibility that exists under the Data Protection Directive and research has shown that the implementation of this varies greatly from state to state. There are some Member States that have not even passed the legislation to implement derogations that were required more than 20 years ago under the DPD.[361] Therefore, it is rather unreasonable to expect the Member States to enact more balanced and effective protections under the GDPR than they did under the DPD.[362]

As a final point, the GDPR introduced a new concept of a one-stop shop mechanism, which is designed to facilitate data processing operations for data controllers that operate in more than one Member State.[363] Under this mechanism, an intermediary that acts as a data controller and has several establishments in several EU Member States would have a single supervisory authority in the country of its main establishment, which would act as the lead authority. The lead authority will be responsible for the oversight of all the processing activities of the controller across the EU.[364] The one-stop shop mechanism together with the consistency measure that requires consultation between the national supervisory authorities in situations where an issue has arisen which involves the processing of personal data of data subjects from several Member States, will ensure consistency between the obligations of controllers in the EU.[365] The idea of greater cooperation between the DPAs of the EU Member States is welcome, but in order for such cooperation to be effective, at least with regard to internet intermediaries, the questions referring to the interpretation of the Article 17 right to erasure need to be clarified.

---

[359] Article 17(3)(a) GDPR
[360] Article 85(1) GDPR
[361] Erdos, D. European Union data protection law and media expression: fundamentally off balance I.C.L.Q. 2016, 65(1), 139-183, at 150
[362] Keller, D. Free Expression Gaps in the General Data Protection Regulation (30 November 2015) https://cyberlaw.stanford.edu/blog/2015/11/free-expression-gaps-general-data-protection-regulation (17.04.2016)
[363] Dor, T. and Rimsevica, D. Changes introduced by the General Data Protection Regulation C.T.L.R. 2016, 22(1), 5-8, at 7
[364] Recital 124 GDPR
[365] Dor and Rimsevica (supra nota ) at 7

### 5.2.2. A Digital Single Market Strategy for Europe

The European Commission committed in its Communication on a Digital Single Market Strategy for Europe of 6 May 2015 to assess the role of online platforms and intermediaries.[366] The Communication stressed the even more central role that online platforms, such as search engines, social media networks, e-commerce platforms, app stores and price comparison websites are playing in social and economic life. Furthermore, platforms have proven to be innovators in the digital economy, for example by helping smaller businesses to move online and reach new markets. On the other hand, the Communication also mentioned the growing concerns over the increasing market power of some platforms resulting from a lack of transparency over their exact use of the information they acquire and their strong bargaining power compared to that of their clients.[367] The Communication also mentioned the e-Commerce Directive and its rules on intermediary liability and reiterated that intermediaries should not be liable for the content that they transmit, store or host, as long as they act in a strictly passive manner and take effective action to remove illegal content when such material is identified. It recognised the problems concerning the disabling of access and the removal of illegal content and made a commitment to analyse the need for new measures to tackle illegal content while also taking into account the impact of online platforms on the fundamental right to freedom of expression and information.[368]

Resulting from this commitment the European Commission launched a public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy. At the time of writing, the final results of the consultation have not yet been published, although the Commission has made available a set of first brief results that outline the preliminary trends observed in the consultation.[369] These give a rather vague overview of some of the concerns relating to intermediaries, such as transparency questions regarding search results and the lack of sufficient information about the personal data collected from individuals. Unsurprisingly, most online platforms think that they do provide enough information on their operations. As to the e-Commerce Directive, views are divided over those who consider the liability regime to still be fit for purpose and those who would like clarification and guidance for

[366] Commission Communication on a Digital Single Market Strategy for Europe (supra nota )
[367] Ibid, para 3.3.1.
[368] Ibid, para 3.3.2.
[369] First brief results of the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy https://ec.europa.eu/digital-single-market/en/news/first-brief-results-public-consultation-regulatory-environment-platforms-online-intermediaries (25.04.2016)

its implementation as well as introducing further categories of intermediary services in addition to mere conduits, caching and hosting providers. Notably, the majority of respondents to the consultation believe that different categories of illegal content need different policy approaches with regard to notice-and-action procedures. There is an understandable difference of opinion between rights holders and enforcement authorities on the one hand, and intermediaries on the other, on the topic of a "take down and stay down" principle for illegal content. In addition to not supporting the "take down and stay down" principle, intermediaries are also reluctant about the idea of introducing specific duties of care for certain categories of illegal content.

## Conclusion

Internet has fundamentally changed the way people can exercise their civil, economic and political rights by providing a forum where one can develop one's social personality and engage in social relationships. However, the role of the internet as a fundamental enabler of individual and social development is not always socially beneficial as evidenced by online defamation, cyberbullying, violations of intellectual property rights, hate speech, child pornography, support of criminal activity and terrorism, etc. Most of such content, whether beneficial or not, is created by individuals acting in their private capacity, but supported by the activities of profit-seeking private companies, who provide the infrastructure necessary for the exercise of their users' rights. It is these intermediaries that are increasingly becoming subjects of claims wishing to hold them accountable for the actions of their users. This trend is evidenced by the recent high-profile cases before the CJEU and the ECtHR.

The primary aim of the present thesis was to examine and determine how current European legislation and case law responds to the issue of intermediary liability, especially in cases involving user-generated content, and to draw comparisons between the different regimes and to analyse their effects. However, before being able to focus on the different legal regimes applicable to intermediary liability, it was necessary to determine what exactly an intermediary is. The definitions vary greatly since the exact functions and roles of intermediaries also differ. Therefore, a broad construction of the term focusing on the functions of intermediaries was adopted for the purposes of the thesis. Thus, the main focus in the present thesis was on internet intermediaries, which facilitate internet-based communications by allowing persons to upload or post their own content on a platform provided by the intermediary.

The legal regimes governing intermediary liability emerged both in Europe and in the United States by the year 2000. While it was recognised that different types of internet service providers perform different functions and require specific responses, they should in principle be guaranteed an exemption, or at least a limited exemption, from liability for content created by third parties. It was agreed that the liability exemptions should commonly consist of two basic principles: immunity for intermediaries for third party content if they do not modify the content nor are aware of its illegal character, and no general obligation to monitor content. In order for intermediaries to

benefit from immunity, they should be prepared to remove or block access to illegal or infringing content when required. In the EU, these principles were enshrined in the e-Commerce Directive.

The overall aim of the e-Commerce Directive was to clarify the position and provide greater legal certainty to intermediary service providers. However, as evidenced by the differing national implementations of the directive as well as the contrasting decisions of both domestic and international courts, the aim was not entirely achieved. Section 4 of the Directive, consisting of Articles 12 to 15, outlines the harmonised regime of the liability exemptions for intermediary service providers throughout the EU. It includes three types of activities – mere conduit, caching and hosting, and contains two types of protection – against liability and monitoring obligations. Accordingly, Articles 12-14 safeguard certain intermediaries against complaints about the transport or storage of information supplied or requested by their users, and Article 15 protects against injunctions and orders requiring them to actively monitor or search their platforms for illegal content.

The second regime governing intermediary liability in Europe is the Data Protection Directive, under which the liability of intermediaries hinges on the question whether they can be classified as either a data controller or data processor. A data controller determines the purposes and means of the processing while a data processor simply processes data on behalf of the controller. For example, a hosting provider is a processor for any personal data distributed online by its users, who use the service for their website hosting and maintenance. In case the hosting provider, however, further processes data contained on the websites for its own purposes, then the host will become a controller with respect to that particular processing. If an intermediary is classified as a controller, then it is subject to the stringent requirements of the DPD.

With regard to the relationship between the e-Commerce Directive and the Data Protection Directive, it has been argued that since the issues concerning the protection of personal data are explicitly excluded from the scope of the ECD, this could lead to the conclusion that a hosting intermediary would be responsible for violations of third parties' data protection rights committed by their users even in situations where the intermediary has engaged in neutral activities and would thus qualify for the liability exemption found in Article 14 of the ECD. On the other hand, however, the above interpretation of the Data Protection Directive, namely that hosting providers will be considered as data processors and not controllers with respect to personal data disclosed by their users, seems to be consistent with the intermediary liability regime in the e-Commerce

Directive. In both cases, as long as a hosting provider deals with content on behalf and according to the instructions of the user of its service, the intermediary remains protected from liability.

The final regime applicable to intermediary liability is freedom of expression, enshrined inter alia, in Article 10 of the ECHR. Unlike with data protection, legal persons, such as companies and associations, can also claim violations of their human rights under the ECHR system. This was confirmed by two judgments of the ECtHR in the *Delfi* and *MTE and Index* cases. Although the cases concerned very similar facts, in Delfi the court found no violation of Article 10 of the ECHR while in *MTE and Index* there was a violation. Both cases concerned comments posted by users on online news portals, but the cases were differentiated on the basis that the comments in *MTE and Index* were merely vulgar and offensive and did not amount to hate speech and incitement to violence like in *Delfi,* which were clearly unlawful on the outset. Differentiating between these two categories of comments will likely be very problematic in practice.

Also in the *MTE and Index* case, the ECtHR crucially held that implementing a NTD system accompanied by effective procedures allowing for rapid response is sufficient to balance the rights and interests of the parties involved. This interpreted in combination with the *Delfi* ruling, means that it is acceptable if offensive comments are deleted upon notification, while higher standards of care need to be applied to hate speech and incitement to violence, which requires portals to remove material on their own initiative. The problem with such an interpretation is, however, that in order to detect hate speech, monitoring of all comments will most likely need to be done. This, in turn, runs the risk of leading into general monitoring, which is explicitly prohibited under Article 15 of the ECD, except in specific cases and with an order by a national court or administrative authority.

Consequently, employees of internet intermediaries looking for *Delfi*-level comments that are clearly unlawful will inevitably come across other user-generated content that might reach *MTE*-level defamation. Despite the fact that according to the ECtHR intermediaries cannot be required to look for the latter, once employees see them, they will presumably be removed as well. This results from the requirement set out in Article 14 of the e-Commerce Directive that once an intermediary gains knowledge of unlawful content, whether via notice or other means, it must expeditiously remove it. By virtue of not being able to assess the truth of the disputed facts, employees of internet intermediaries are put into an impossibly difficult position to make legal judgments that even courts find complicated. This will most likely lead to over removal of content just to be safe and avoid liability. This will in turn lead into so-called private censorship meaning

the burden of establishing whether that content really is illegal or not is on private companies instead of state authorities. The conclusion then seems to be that Articles 14 and 15 of the ECD offer online intermediaries more protection than both the Data Protection Directive and the right to freedom of expression in Article 10 of the ECHR. Thus, the hypothesis of the thesis, which was that the current state of intermediary liability for user-generated content in the European legal order is extremely unclear since there are three separate and conflicting regimes that simultaneously govern the issue, seems to be true.

To conclude, the current situation in Europe regarding the liability of internet intermediaries in Europe is extremely unclear and confusing. The only hope is that the EU consultations on online platforms will lead to the adoption of new uniform approach to intermediary liability. However, judging from the experience of the adoption of the GDPR, it is very likely that such a uniform liability regime is far from happening any time soon.

## Kokkuvõte

Käesoleva magistritöö teema valik on ajendatud tänapäeval väga aktuaalsest ja rohkesti tähelepanu pälvinud probleemist, nimelt kas infoühiskonna teenuse vahendajad peaksid vastutama nende kasutajate loodud sisu eest.

Magistritöö hüpoteesiks oli väide, et hetkel on Euroopas kolm erinevat õiguslikku reziimi, mis reguleerivad infoühiskonna teenuse vahendajate vastutust nende kasutajate loodud sisu eest. Nendeks on e-kaubanduse direktiiv, andmekaitse direktiiv ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis sisalduv sõnavabadus.

Töö eesmärk oli analüüsida õiguslikust aspektist eelpool mainitud kolme reziimi, uurides erinevaid Euroopa õigusakte ning kohtu lahendeid. Analüüsi põhjal ilmnes, et kuigi käesolevad kolm reziimi kattuvad teatud määral, on nende vahel ka märgatavaid erinevusi.

E-kaubanduse direktiivi alusel pääsevad infoühiskonna teenuse vahendajad enamustel juhtudel vastutusest kui nad ei ole teadlikud nende platvormidel asuvast ebaseaduslikust sisust. Artikkel 10 sõnavabaduse alusel ei piisa aga sisu eemaldamisest juhul kui tegemist on vihakõnega ning kõnega, mis õhutab vaenu, kuid kui tegemist on lihtsalt ebaviisaka sisu või laimuga, piisab samuti eemaldamisest, et vältida vastutusest tulenevaid tagajärgi. Andmekaitse direktiivi puhul, aga oleneb vastutus sellest, kas infoühiskonna teenuse vahendajat võib klassifitseerida volitatud töötlejana või vastutava töötlejana. Viimasel juhul peab teenuse vahendaja rakendama kõiki direktiivis toodud nõudeid ning Google Hispaania kaasusest tulenevalt ka olema valmis teatud juhtudel andmeid kustutama.

Kokkuvõttes, on praegu Euroopas valitsev infoühiskonna teenuse vahendajate vastutust reguleeriv reziim äärmiselt ebaselge, mis on omakorda tekitanud erinevate riikide kohtupraktikas väga vastakaid lahendeid. Tuleb loota, et Euroopa tasandil hiljuti vastu võetud andmekaitse reform ja ka plaanis olev infoühiskonna teenuse vahendajate reform toovad teemasse selgust.

# Bibliography

## Books and Journal Articles


1) Alston, P. & Goodman, R. International Human Rights – Text and Materials. 1st edn. Oxford: Oxford University Press 2013
2) Arnold, R. Website-blocking injunctions: the question of legislative basis (2015) E.I.P.R. 37(10), pp. 623-630
3) Azevedo Cunha, M. V., Marin, L. & Sartor, G. Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web (2012) International Data Privacy Law, Vol. 2, No. 2, pp. 50-67
4) Barata Mir, J. & Bassini, M. Freedom of Expression in the Internet – Main Trends of the Case Law of the ECtHR. In Pollicino, O. & Rome, G. (eds.) The Internet and Constitutional Law: The Protection of Fundamental Rights and Constitutional Adjudication in Europe. Oxford: Routledge 2016
5) Carey, P. Data Protection: A Practical Guide to UK and EU Law. 3rd edn. Oxford: OUP 2009
6) Castells, M. Communication Power. Oxford: OUP 2009
7) Cornthwaite, J. To key or not to key? The judgment of the European Court of Justice in the Google France Adwords cases. E.I.P.R. 2010, 32(7), 352-359
8) Cox, N. Delfi AS v Estonia: The Liability of Secondary Internet Publishers for Violation of Reputational Rights under the European Convention on Human Rights (2014) 77(4) MLR pp. 619-640
9) Crowther, H. Remember to forget me: the recent ruling in Google v AEPD and Costeja Gonzales (2014) Computer and Telecommunications Law Review, 20(6), pp. 163-165
10) Dor, T. and Rimsevica, D. Changes introduced by the General Data Protection Regulation C.T.L.R. 2016, 22(1), 5-8
11) Edwards, L. Privacy and Data Protection Online: The Laws Don't Work. In Edwards, L. & Waelde, C. (eds) Law and the Internet. 3rd edn. Portland: Hart Publishing 2009
12) Edwards, L. The Fall and Rise of Intermediary Liability Online. In Edwards, L. & Waelde, C. (eds) Law and the Internet. 3rd edn. Portland: Hart Publishing 2009
13) Erdos, D. European Union data protection law and media expression: fundamentally off balance I.C.L.Q. 2016, 65(1), 139-183

14) Frantziou, E. Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos (2014) Human Rights Law Review, 14, pp. 761–777
15) Gellert, R. & Gutwirth, S. The legal construction of privacy and data protection (2013) Computer Law and Security Review 29, pp. 522-530
16) Gillen, M. Human versus Inalienable Rights: Is there still a future for online protest in the Anonymous world? (2012) European Journal for Law and Technology, Vol. 3, No. 1.
17) Greenberg, M.H. A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market, 18 Berkeley Tech. L.J. (2003) pp. 1191-1258
18) Hurst, A. Data privacy and intermediary liability: striking a balance between privacy, reputation, innovation and freedom of expression. Ent. L.R. 2015, 26(6), 187-195
19) Jondet, N. France: EC Directive 2000/31 of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, art.14; Act on Confidence in the Digital Environment of 21 June 2004, art.6-I-2 and 5 - "Nord-Ouest v Dailymotion". IIC 2012, 43(5), 614-617
20) Julià-Barceló, R. and Koelman, K.J. Intermediary Liability In The e-Commerce Directive: So Far So Good, But It's Not Enough, Computer Law & Security Review, 16 (2004) 4, 231–239
21) Jääskinen, N. The Place of the EU Charter within the Tradition of Fundamental and Human Rights. In (eds) Morano-Foadi, S. and Vickers, L. Fundamental Rights in the EU: A Matter for Two Courts. Oxford: Hart Publishing 2015
22) Kuczerawy, A. Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative, Computer Law & Security Review 31 (2015) 46-56
23) Lynskey, O. Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order. I.C.L.Q. 2014, 63(3), 569-597
24) Marsoof, A. Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression (2011) International Journal of Law and Information Technology Vol. 19 No. 2, pp. 110-132
25) McCarthy, H.J. Is The Writing on the Wall for Online Service Providers? Liability For Hosting Defamatory User-Generated Content Under European and Irish Law. 14 Hibernian L.J. 16 2015, 16-55
26) McGoldrick, D. Developments in the Right to be Forgotten (2013) 13 Human Rights Law Review 761-766
27) Mlynar, V. A Storm in ISP Safe Harbour Provisions: The Shift from Requiring Passive-Reactive to Active-Preventative Behaviour and Back. (2014) 19 Intell. Prop. L. Bull. 1

28) Oliver, P. Companies and their fundamental rights: a comparative perspective I.C.L.Q. 2015, 64(3), 661-696
29) Peguera, M. "I just know that I (actually) know nothing": actual knowledge and other problems in ISP liability case law in Spain. E.I.P.R. 2008, 30(7), 280-285
30) Rantou, M. The growing tension between copyright and personal data protection on an online environment: The position of Internet Service Providers according to the European Court of Justice (2012) European Journal for Law and Technology, Vol. 3, No. 2.
31) Reed, C. Policies for Internet Immunity. 2009 Computers and Law, Vol. 19(6), 20
32) Sartor, G. Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? International Data Privacy Law, 2013, Vol. 3, No. 1, pp. 3-12
33) Tapscott, D. & Williams, A.D. Wikinomics: How Mass Collaboration Changes Everything. New York: Penguin New York 2008
34) Tracol, X. Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it. Computer Law & Security Review 31 (2015) 112-119
35) Van Eecke, P. Online Service Providers and Liability: A Plea for a Balanced Approach. Common Market Law Review 48: 1455-1502, 2011
36) Van der Sloot, B. Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe, 6 (2015) JIPITEC 211, pp. 211-228
37) Van Kempen, P. Human Rights and Criminal Justice Applied to Legal Persons. Protection and Liability of Private and Public Juristic Entities under the ICCPR, ECHR, ACHR and AfChHPR. Electronic Journal of Comparative Law, vol. 14.3 (December 2010), http://www.ejcl.org/143/art143-20.pdf (12.03.2016)
38) Varadi, S., Kertesz, A. and Parkin, M., The necessity of legally compliant data management in European cloud architectures. C.L.S.R. 28 (2012) 577-586
39) Warso, Z. There's more to it than data protection: Fundamental rights, privacy and the personal/household exemption in the digital age. Computer Law and Security Review 29 (2013) 491-500
40) Weinert, E. MTE v Hungary: the first European Court of Human Rights ruling on liability for user comments after Delfi AS v Estonia. Ent. L.R. 2016, 27(4), 135-139
41) Zittrain, J. A History of Online Gatekeeping, Harvard Journal of Law and Technology, Vol. 19, No. 2, 2006, p.253-298

**Legislation**

- Charter of Fundamental Rights of the European Union
- European Convention for the Protection of Human Rights and Fundamental Freedoms International Covenant for Civil and Political Rights
- Treaty on the European Union (*Articles 5(4) & 6*)
- Universal Declaration of Human Rights
- 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, OJ L 281, 23.11.1995, p 0031-0050
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002 p 0037-0047
- Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 195, 02.06.2004 p 0016-0025
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337/11, 18.12.2009 p 0011-0036
- Regulation (EU) 2016/… of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

**Case Law**

***Court of Justice of the European Union***

- Case C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971
- Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-00271

- Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECR I-09831
- Joined cases C-236/08 to C-238/08 *Google France SARL v Louis Vuitton Malletier SA; Google France SARL v Viaticum SA et al; Google France SARL v CNRRH SARL et al* [2010] ECR I-02417
- Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063
- Case C-324/09, *L'Oréal SA and Others v eBay International AG and Others* [2011] ECR I-06011
- Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2010] ECR I-11959
- Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [2012] ECLI:EU:C:85
- Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:317
- Joined Cases C-141/12 and C-372/12 *YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M, S,* [2014] ECLI:EU:C:2081, Opinion of Advocate General Sharpston
- Case C-291/13 *Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd and Others* [2014] ECLI:EU:C:2209

***European Court of Human Rights***

- Application no. 5493/72, *Handyside v the United Kingdom* (7 December 1976)
- Application no. 23144/93, *Özgur Gündem v Turkey* (16 March 2000)
- Application no. 2872/02, *K.U. v Finland* (2 December 2008)
- Application nos. 3002/03 and 23676/03, *Times Newspapers Ltd. (nos. 1 and 2) v United Kingdom* (10 March 2009)
- Application no. 33014/05, *Editorial Board of Pravoye Delo and Shtekel v Ukraine* (5 May 2011)
- Application no. 33846/07, *Wegrzynowski and Smolczewski v Poland* (16 July 2013)
- Applications nos. 40660/08 and 60641/08, *Von Hannover v Germany (No. 2)* (7 February 2012)

- Application no. 48009/08, *Max Mosley v UK* (10 May 2011)
- Application no. 3111/10, *Ahmet Yildirim v Turkey* (18 December 2012)
- Application no. 64569/09, *Delfi AS v Estonia* (16 June 2015)
- Application no. 22947/13, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu ZRT v Hungary* (2 February 2016)

***National Courts***

- *Byrne v Deane* [1937] 1 KB 818 (England & Wales Court of Appeal, King's Bench Division)
- *CG v Facebook Ireland Ltd* [2015] NIQB 11 (Northern Ireland High Court, Queen's Bench division)
- *Godfrey v Demon Internet Ltd* [2001] QB 201 (England & Wales High Court, Queen's Bench Division)
- *Imran Karim v Newsquest Media Group Limited* (Unreported, 27 October 2009; England & Wales High Court, Queen's Bench Division)
- *J19 v Facebook Ireland* [2013] NIQB 113 (Northern Ireland High Court, Queen's Bench division)
- *Kaschke v Hilton* [2010] EWHC 690 (England & Wales High Court, Queen's Bench Division)
- *Mosley v Google Inc* [2015] EWHC 59 (QB
- *Mulvaney v The Sporting Exchange Trading as Betfair* [2009] IEHC 133 (Ireland High Court)
- *Tamiz v Google Inc* [2013] EWCA Civ 68 (England & Wales Court of Appeal, Civil Division)
- *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB)
- *Vjatšeslav Leedo v AS Delfi* (Case no. 3-2-1-43-09, Estonian Supreme Court, 10 June 2009)

**International Organisations – Reports, Consultations, Communications, Working Papers**

- Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Opinion 1/2010 on the concepts of "controller" and "processor". (Adopted on 16 February 2010) WP 169, 00264/10/EN http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf
- Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data. Opinion 1/2008 on data protection issues related to search engines. (Adopted

on 4 April 2008) 00737/EN WP 148 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf

- Copenhagen Economics. Study on the impact of online intermediaries on the EU economy (April 2013) https://www.copenhageneconomics.com/dyn/resources/Publication/publicationPDF/6/226/0/The%20impact%20of%20online%20intermediaries%20-%20April%202013.pdf
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, Brussels, 6.5.2015, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=EN
- European Commission Communication to the European Parliament, The Council, The Economic and Social Committee and The Committee of Regions. A coherent framework for building trust in the Digital Single Market for e-Commerce and online services (SEC(2011) 1640 final, http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/COM2011_942_en.pdf)
- European Commission Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, COM(2013) 627 final 2013/0309 (COD)
- First brief results of the public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy https://ec.europa.eu/digital-single-market/en/news/first-brief-results-public-consultation-regulatory-environment-platforms-online-intermediaries
- Internet intermediaries: Dilemma of Liability, Article 19, https://www.article19.org/data/files/Intermediaries_ENGLISH.pdf
- The Economic and Social Role of Internet Intermediaries, OECD April 2010, http://www.oecd.org/internet/ieconomy/44949023.pdf
- OECD Report on the Economic and Social Role of Internet Intermediaries (2010 http://www.oecd.org/internet/ieconomy/44949023.pdf
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye on the use of encryption and anonymity in digital communications (A/HRC/29/32, 22 May 2015) http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue on the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet (A/HRC/17/27, 16 May 2011) http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Research Division of the European Court of Human Rights. Internet: case-law of the European Court of Human Rights. www.echr.coe.int/Documents/Research_report_internet_ENG.pdf
- Verbiest, Spindler, Riccio and Van der Perre, Study on liability of Internet intermediaries (study prepared for the European Commission - Markt/2006/09/E Service Contract ETD/2006/IM/E2/69) (12 November 2007) http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf
- World Editors Forum Report on Online comment moderation: emerging best practices – A guide to promoting robust and civil online conversation (2013-10-04) http://www.wan-ifra.org/reports/2013/10/04/online-comment-moderation-emerging-best-practices


**Other Sources**


- Annual revenue of Google from 2002 to 2015: http://www.statista.com/statistics/266206/googles-annual-global-revenue/
- Barlow, J.P. A Declaration of the Independence of Cyberspace (Davos, February 8, 1996) https://www.eff.org/cyberspace-independence
- English, R. UK Human Rights Blog: Internet trolls and why Strasbourg doesn't want to get involved (14 October 2013) http://ukhumanrightsblog.com/2013/10/14/internet-trolls-and-why-strasbourg-doesnt-want-to-get-involved/
- ERR Online. Isikutuvastamine ERR.ee kommentaariumis on nüüd ühekordne, end tuvastada saab ka mobiil-ID-ga (29 January 2016) http://uudised.err.ee/v/eesti/d631cdc9-8393-4fc1-8fd7-96f5260c7d41/isikutuvastamine-erree-kommentaariumis-on-nuud-uhekordne-end-tuvastada-saab-ka-mobiil-id-ga
- European Parliament Press Release: Data protection reform - Parliament approves new rules fit for the digital era (14 April 2016) http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era

- Goodman, E. Is Anonymous Commenting Under Threat in the EU? (23 October 2013) http://blogs.lse.ac.uk/mediapolicyproject/2013/10/23/is-anonymous-commenting-under-threat-in-the-eu/
- Griffiths, R. Normality restored: website hosts may again be liable for defamatory user generated content (19 February 2013) http://www.fieldfisher.com/publications/2013/02/normality-restored-website-hosts-may-again-be-liable-for-defamatory-user-generated-content#sthash.N3zfDajq.dpbs
- Hodson, H. Apple vs FBI: Who will win this struggle for power? (New Scientist, 22 February 2016) https://www.newscientist.com/article/2078419-apple-vs-fbi-who-will-win-this-struggle-for-power/
- Kangro, K. Postimees sulgeb veebruarist anonüümse kommentaariumi (30 December 2015) http://www.postimees.ee/3451469/postimees-sulgeb-veebruarist-anonuumse-kommentaariumi
- Keller, D. Free Expression Gaps in the General Data Protection Regulation (30 November 2015) https://cyberlaw.stanford.edu/blog/2015/11/free-expression-gaps-general-data-protection-regulation
- Keller, D. Policing Online Comments in Europe: New Human Rights Case Law in the Real World (12 April 2016) https://cyberlaw.stanford.edu/blog/2016/04/policing-online-comments-europe-new-human-rights-case-law-real-world
- Keller, D. The Final Draft of Europe's "Right to Be Forgotten" Law (17 December 2015) http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law
- Kuczerawy, A. and Ombelet, P.J. Reconciling Delfi vs. Estonia with EU rules on intermediary Liability http://blogs.lse.ac.uk/mediapolicyproject/2015/07/01/not-so-different-after-all-reconciling-delfi-vs-estonia-with-eu-rules-on-intermediary-liability/
- Malcomson, S. Growing up: How the internet lost its free spirit (The Economist, 26 March 2016) http://www.economist.com/news/books-and-arts/21695370-how-internet-lost-its-free-spirit-growing-up
- Metz, C. How Google's New Wireless Service Will Change the Internet. WIRED Magazine (3 March 2015) www.wired.com/2015/03/googles-new-wireless-service-will-change-internet/
- Ombelet, P.J. and Kuczerawy, A. Delfi revisited: the MTE-Index.hu v. Hungary case (February 2016) http://blogs.lse.ac.uk/mediapolicyproject/2016/02/19/delfi-revisited-the-mte-index-hu-v-hungary-case/
- Stalla-Bourdillon, S. Internet intermediaries: How are you? What do you do? What the European Commission has to say (14 September 2015), available at

https://peepbeep.wordpress.com/2015/09/14/internet-intermediaries-how-are-you-what-do-you-do-what-the-european-commission-has-to-say/

- Voorhoof, Dirk. Delfi AS v. Estonia: Grand Chamber confirms liability of online news portal for offensive comments posted by its readers (18 June 2015) http://strasbourgobservers.com/2015/06/18/delfi-as-v-estonia-grand-chamber-confirms-liability-of-online-news-portal-for-offensive-comments-posted-by-its-readers/
- Walzel, S. European Commission Consults on Notice and Takedown (24 August 2012) http://blogs.lse.ac.uk/mediapolicyproject/2012/08/24/european-commission-consults-on-notice-and-takedown/
- Woods, Lorna. Delfi v Estonia: Curtailing online freedom of expression? (18 June 2015) http://eulawanalysis.blogspot.com.ee/2015/06/delfi-v-estonia-curtailing-online.html